Common Criteria Configuration and Administration Guide

Setting up and administrating the Common Criteria configuration using Mac OS X or Mac OS X Server

Version 1.0.1

Apple Computer, Inc.
© 2005 Apple Computer, Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X or Mac OS X Server software may reproduce this publication for the purpose of learning to use such software. No part of this publication may be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid for support services.

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AppleScript, AppleShare, AppleTalk, FireWire, iBook, iMac, Mac, Macintosh, Mac OS, Power Book, Power Mac, Power Macintosh, QuickTime, and Xserve are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.eMac and Finder are trademarks of Apple Computer, Inc.

PowerPC is a trademark of International Business Machines, Incorporated, used under license therefrom.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

019-0409/04-05-2005

Version 1.0.1

Contents

Preface 7 **Document Revision History**

Chapter 1 9 **The Common Criteria Configuration**
9 About Common Criteria
10 Assumptions About the Environment of the Configuration
11 Assumptions About the Usage of the Common Criteria Configuration
11 How to Use This Guide
11 Getting Additional Information

Chapter 2 13 **Installing Common Criteria with Mac OS X or Mac OS X Server**
13 Installing the Latest version of Mac OS X
17 Installing the Evaluated Configuration of Mac OS X
20 Installing the Latest version of Mac OS X Server
24 Installing the Evaluated Configuration of Mac OS X Server

Chapter 3 29 **Setting Up the Common Criteria Configuration**
29 Set Up System Preferences
29 Security
29 Screen Saver
30 CDs & DVDs
30 Sharing
30 Accounts
31 Date & Time
31 Energy Saver
31 System Setup
31 Directory Access
31 Set an Open Firmware Password
33 Turn On Auditing
33 Disable Password Hints
34 Set Password Policy
34 Set the Global umask
34 Configure Secure Shell
35 Remove Classic
36 Restart

Chapter 4 37 **Using Mac OS X in a Secure Manner**
37 Using Passwords in Mac OS X
37 Choosing Good Passwords
38 Logging Out at the End of a Session
38 Setting the umask for Individual Users
39 Setting Permissions for Disks, Folders, and Files
40 Setting Permissions in the Mac OS X interface
40 Setting Permissions Using UNIX Commands
40 Understanding UNIX Permissions
41 Changing Permissions
42 Changing the Owner
43 Changing the Group

Chapter 5 45 **Administering Mac OS X in the Common Criteria Configuration**
45 Managing Audit Log Files
46 About Administrator Accounts
46 Adding a New User Account
47 Changing a Password
47 Deleting a User Account
47 Setting the Default Permissions for New Files
48 Set Password Policy
48 Administering User and Group Accounts With UNIX Commands
49 Adding a User Account via the Command Line
52 Removing a User Account via the Command Line
53 Modifying a user Account via the Command Line
53 Adding a New Group via the Command Line
55 Removing a Group via the Command Line
55 Adding a user to a Group via the Command Line
56 Removing a User from a Group via the Command Line
57 Revoking a User's Right to Access the System
57 Preventing Users From Logging In
59 Terminating All of a User's Processes

Chapter 6 61 **Mac OS X Auditing Administrator's Guide**
61 The Audit Utility
62 Audit Startup
62 Audit Classes, Audit Events, and User Masks
63 Command-Line Programs
63 audit
64 auditreduce
65 praudit
67 Deleting Audit Records
67 Audit Control Files

67 audit_class
67 audit_control
69 audit_event
69 audit_user
70 audit_warn
71 Audit Log Files
71 Modifying the Audit System

Appendix A 73 **Common Criteria Setup Checklist**
73 Checklist
73 Security
74 Screen Saver
74 CDs & DVDs
74 Sharing
75 Accounts
75 Date & Time
75 Energy Saver
75 Directory Access
76 Set an Open Firmware Password
76 Turn On Auditing
76 Disable Password Hints
77 Set Password Policy
77 Set the Global umask
78 Configure Secure Shell
78 Remove Classic
78 Restart

Appendix B 79 **Mac OS X Audit Event Classes**

Appendix C 81 **Audit Record Format**

Appendix D 101 **Satisfying CAPP Requirements**

Appendix E 103 **Using Terminal**
103 Notation Conventions
103 Summary
103 Commands and Other Terminal Text
104 Command Parameters and Options
104 Using Terminal
105 Correcting Typing Errors
105 Repeating Commands
105 Including Paths Using Drag-and-Drop
105 Commands Requiring Root or Administrator Privileges
106 Getting Online Help for Commands

106 Editing Settings Files

Appendix F 107 CAPP Requirements for the Audit Tools

Document Revision History

This table describes revisions to the Common Criteria Administration Guide.

Date	Notes
April 2, 2005	• Modified instructions for setting the global umask to account for differences in certain Panther configurations. This command has been added to pages 32 and 75: sudo chmod 644 /Library/Preferences/.GlobalPreferences.plist • Added change history page.

The Common Criteria Configuration

1

This guide provides the information needed to set up, use, and administer Mac OS X and Mac OS X Server in compliance with the Common Criteria specification.

About Common Criteria

Common Criteria is an international standard that helps to ensure the security of computer systems in a network environment. You can optimize the security of your network by bringing each system into conformance with the standard defined by Common Criteria. To do so you must ensure that the hardware and software settings of each system match the specific configuration evaluated and certified as secure by the Common Criteria specification. The Common Criteria evaluation for Mac OS X and Mac OS X Server was performed with a configuration referred to in this document as the *evaluated configuration*.

The evaluated configuration consists of:

- Mac OS X version 10.3.6 with the Common Criteria Tools version 1.0, installed on any of the following computers: eMac, iBook, iMac, PowerBook, or Power Mac with a single or dual PowerPC G3, G4, or G5 processor.
- Mac OS X Server version 10.3.6 with the Common Criteria Tools version 1.0, installed on any of the following computers: eMac, iMac, Power Mac, PowerBook, iBook, or Xserve with a single or dual G3, G4, or G5 processor.

All Common Criteria functionality has been incorporated into Mac OS X starting with Mac OS X version 10.3.6 and Mac OS X Server version 10.3.6.

Important: It's recommended that you use the latest version of Mac OS X or Mac OS X Server to benefit from the most recent security and system enhancements.

You only need to use the version10.3.6 to duplicate the exact system environment that was evaluated for Common Criteria compliance.

A computer with the *Common Criteria configuration* may be using a newer version of Mac OS X, but otherwise shares all the system settings included in the evaluated configuration.

Note: Do not install Mac OS 9 (the Classic environment) or any operating system other than Mac OS X or Mac OS X Server on the Common Criteria configuration.

The Common Criteria configuration includes one or more of the above computers connected to a local network via Ethernet. It can also include connected peripheral devices including the following:

- Display
- Keyboard
- Mouse
- CD-ROM drive
- DVD-ROM drive
- Fixed disk drives
- Printer
- Audio Adapter
- Network Adapter

Assumptions About the Environment of the Configuration

Several assumptions are made about the physical environment of the Common Criteria configuration.

- The hardware must be located within controlled access facilities that prevent unauthorized physical access, and must be protected from unauthorized physical modification.
- All systems with which the Common Criteria configuration communicates, and the communication paths themselves, are assumed to be under the same management as the Common Criteria configuration and abide by the same security policies.
- Any network connections, equipment, and cables in the environment are appropriately protected.
- All connections to peripheral devices reside within the controlled access facilities. Internal communication paths to access points such as terminals are assumed to be adequately protected.

Assumptions About the Usage of the Common Criteria Configuration

The Common Criteria configuration is assured to provide effective security measures in a cooperative, non-hostile environment only if it is installed, managed, and used in accordance with the instructions in this guide. The following conditions are assumed to exist in the environment where the Common Criteria configuration is employed:

- There will be one or more competent individuals assigned to manage the Common Criteria configuration and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided in this guide.
- Authorized users possess the necessary authorization to access at least some of the information managed by the Common Criteria configuration and are expected to act in a manner that contributes to the security of the environment and the information it contains.

How to Use This Guide

To use the Common Criteria configuration, you must install the required software and set up the software according to the Common Criteria specification. See Chapters 2 and 3 for instructions.

Next, see Chapter 4 for information on using your systems in a safe and secure way.

Finally, Chapters 5 and 6 have information on administering the Common Criteria configuration, including instructions for using the command line to do management tasks.

Getting Additional Information

Mac OS X and Mac OS X Server come with guides that explain their features and provide instructions on configuring, managing, and troubleshooting them. All of the guides are available as PDF files from http://www.info.apple.com.

This guide	Tells you how to
Mac OS X Panther v10.3 Installation and Setup Guide	Install and set up Mac OS X.
Mac OS X Server Getting Started for Version 10.3 or Later	Get to know the features of Mac OS X Server and do initial setup.
Mac OS X Server User Management for Version 10.3 or Later	Create and manage user, group, and computer accounts and set up managed preferences and Mac OS X clients.
Mac OS X Server File Services Administration for Version 10.3 or Later	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB/CIFS.

This guide	Tells you how to
Mac OS X Server Web Technologies Administration for Version 10.3 or Later	Set up and manage a web server, including WebDAV, WebMail, and web modules.
Mac OS X Server Network Services Administration for Version 10.3 or Later	Set up, configure, and administer services on the server.
Mac OS X Server Open Directory Administration for Version 10.3 or Later	Manage directory and authentication services.
Mac OS X Server Command-Line Administration for Version 10.3 or Later	Use commands and configuration files to perform server administration tasks in a UNIX command shell. Using IP failover is documented in this guide.

Additional information is available at these locations on the web:

- Apple Security Website:
  http://www.apple.com/support/security/
- Science Applications International Corporation (SAIC) evaluation lab website:
  http://www.saic.com/securebiz/cctl.html
- National Information Assurance Partnership (NIAP) website:
  http://niap.nist.gov/
- Apple Documentation
  http://www.apple.com/support/

Installing Common Criteria with Mac OS X or Mac OS X Server

2

This chapter describes how to install the software needed to operate a Macintosh computer in the Common Criteria configuration.

The procedure you need to follow depends on whether you're setting up Mac OS X or Mac OS X Server, and whether you're setting up the latest version of the OS or the exact version used to certify the evaluated configuration.

See the table below for information on what to do:

If you want to install	You need to	For instructions, see
Common Criteria and the latest version of Mac OS X	Install the latest version of Mac OS X and install Common Criteria Tools.	"Installing the Latest version of Mac OS X" on page 13
Mac OS X exactly as used to certify the evaluated configuration	Install Mac OS X version 10.3, update it to version 10.3.6, and install the Common Criteria Tools.	"Installing the Evaluated Configuration of Mac OS X" on page 17
Common Criteria and the latest version of Mac OS X Server	Install the latest version of Mac OS X Server and install Common Criteria Tools.	"Installing the Latest version of Mac OS X Server" on page 20
Mac OS X Server exactly as used to certify the evaluated configuration	Install Mac OS X Server version 10.3, update it to version 10.3.6, and install the Common Criteria Tools.	"Installing the Evaluated Configuration of Mac OS X Server" on page 24

Installing the Latest version of Mac OS X

The instructions in this section tell you how to install the software needed to operate Mac OS X version 10.3.6 or later with the Common Criteria Tools.

What You Need

You need the following installation software to the latest version of Mac OS X and install the Common Criteria Tools:

- **Installation discs for Mac OS X version 10.3 or later**

Use the installation discs included with your system or with your copy of Mac OS X. (You'll update to the latest version of Mac OS X during the following procedure.)

Note: If your installation discs are for a Mac OS X version earlier than 10.3, you must obtain Mac OS X version 10.3 or later.

- **Common Criteria Tools disk image file**
  The Common Criteria Tools disk image (.dmg) file contains the installer for Common Criteria Tools. This disk image file is available from the Common Criteria webpage of the AppleCare Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  After downloading the Common Criteria Tools disk image file, copy it to a removable disk such as a CD-R disc, FireWire disk, or USB disk. For instructions on copying files to a recordable CD or DVD disc, search Mac Help for "Creating CDs and DVDs using the Finder."

Verifying Disk Images

To ensure the disk images you download are accurate, they include an SHA-1 checksum. If a file is changed during transit, its checksum will be different. The SHA-1 digest numbers are listed on the Apple Download web page about the software.

To verify a software update from Apple that contains an SHA-1 digest:

1. Open Terminal.
2. Type the following:

   ```
   /usr/bin/openssl sha1 [full path to file]
   ```

   Example:

   ```
   /usr/bin/openssl sha1 /[full path to file]/1024SecUpd2003-03-03.dmg
   ```

   The SHA-1 digest is displayed as:

   ```
   sha1 ([full path to the file])= [digest]
   ```

   Example:

   ```
   SHA1(/Users/test/Documents/1024SecUpd2003-03-03.dmg)
       =2eb722f340d4e57aa79bb5422b94d556888cbf38
   ```

3. Compare the digest from the Apple web page with the digest of the downloaded image to make sure they match.

   For more information, see this article on the Apple Knowledge Base:
   http://docs.info.apple.com/article.html?artnum=75510

Step 1: Install Mac OS X software

Use the installation discs for Mac OS X version 10.3 or later to install the software.

Important: If you are installing over a previously used system, Apple recommends that you back up the data on your hard disk before you install system software. Apple is not responsible for any lost data.

To install Mac OS X:

1. Turn on the computer and insert the first Mac OS X install disc.
2. Restart the computer while holding down the C key.

   The computer starts up from the install disc. You can release the C key when you see the Apple logo.
3. Proceed through the Installer's panes by following the onscreen instructions.
4. When the Select Destination pane appears, select the volume where you want to install Mac OS X.
5. Click Options, then click Erase and Install.

   The destination volume will be completely erased before Mac OS X is installed on it.
6. Choose Mac OS Extended (Journaled) from the "Format disk as:" pop-up menu.
7. The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc when prompted.

Step 2: Perform initial setup using Setup Assistant

The Setup Assistant program opens automatically when you first start up after you install Mac OS X version 10.3 or later. Setup Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.

Step 3: Update to the latest version of Mac OS X

Apple periodically releases free updates to Mac OS X. In this section you will update to the latest version of Mac OS X. Use one of the two procedures that follow depending on whether the system you're setting up currently has Internet access or not.

- If the computer has Internet access, follow the first procedure. You'll use the Software Update feature to retrieve and install the latest update.
- If the system doesn't have Internet access, follow the second procedure. You'll use another computer to download the software update disk image file, copy it to a removable disk, and use this disk to install the update.

To update Mac OS X on a computer with Internet access:

1. Start up your computer and log in using the name and password of an administrator account.
2. Choose Apple () > Software Update.

   If there are any updates available, they appear in a list.
3. If a Mac OS X update is listed, click its checkbox to select it, then click Install.

Before clicking Install, you can select the checkboxes of other updates you want to install. Apple recommends selecting security updates. To see more information about a particular update, click its name.

When the installation complete, Software Update checks the software versions again. Sometimes several updates are required before the latest version is reached.

After you finish using Software Update, continue with step 4, "Install the Common Criteria Tools software."

To update Mac OS X on a computer without Internet access:

1. On a computer with Internet access, download the disk image file for the latest Mac OS X update from the Apple Support website, then copy the file to a removable disk that's compatible with the system you're setting up.

   You can get the disk image file for the latest update from the Mac OS X Support webpage, which you can get to from the Apple Support website at the following address:

   http://www.apple.com/support/

2. Insert the disk that contains the disk image file for the latest Mac OS X update and open the file to mount the volume containing the update Installer.
3. After the volume is mounted and opens, open the update Installer, which is a package (.pkg) file.
4. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password an administrator account on the computer.
5. After installation is complete, click Restart and continue with the next step.

Step 4: Install the Common Criteria Tools software

After updating your Mac OS software install the Common Criteria Tools.

To install the Common Criteria Tools software:

1. Insert the disk that contains the Common Criteria Tools disk image file and open the file to mount the volume containing the tools Installer.
2. After the volume is mounted and opens, open the Common Criteria Tools Installer, which is a .pkg file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password of the administrator account you created during installation of Mac OS X.
4. Follow the instructions in Chapter 3, "Setting Up the Common Criteria Configuration," on page 29.

Installing the Evaluated Configuration of Mac OS X

The instructions in this section tell you how to install the specific version of Mac OS X used to certify the evaluated configuration. This is only needed to satisfy any requirements to test the specific configuration. It's recommended that you use the latest version of Mac OS X. For more information on the evaluated configuration, see Chapter 1, "The Common Criteria Configuration," on page 9.

What You Need

You need the following installation disks to install the specific version of Mac OS X used to certify the evaluated configuration:

- **Mac OS X version 10.3 (Panther) installation disks**
  You need the either the Mac OS X 10.3 (Panther) or the Mac OS X 10.3.5 (Panther) installation disks. If your computer shipped with Mac OS X 10.3, 10.3.1, 10.3.2,10.3.3, 10.3.4, or 10.3.5 you can use the installation disks that came with your system.
- **Mac OS X 10.3.6 update disk image file**
  To update Mac OS X 10.3, 10.3.1,10.3.2, 10.3.4 to Mac OS X 10.3.6 you need the MacOSXUpdateCombo10.3.6.dmg image file.

  To update Mac OS X 10.3.5 to Mac OS X 10.3.6 use the MacOSXUpdate10.3.6.dmg image file.

  You can determine where to get this file by referring to the Common Criteria webpage of the Apple Care Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  If the Mac OS X Update Installer runs automatically when you download this file, close the Install Mac OS X Update window. If a dialog appears and prevents you from closing the window, click Cancel to dismiss the dialog.

  After downloading the update image file, copy it to a removable disk such as a CD-R disc, FireWire disk, or USB disk. For instructions on copying files to a recordable CD or DVD disc, search Mac Help for "Creating CDs and DVDs using the Finder."
- **Common Criteria Tools disk image file**
  The Common Criteria Tools disk image (.dmg) file contains the installer for Common Criteria Tools. This disk image file is available from the Common Criteria webpage of the AppleCare Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  After downloading the Common Criteria Tools disk image file, copy it to a removable disk.

Verifying Disk Images

To ensure the disk images you download are accurate, they include a SHA-1 digest. If a file is changed during transit, its checksum will be different. The SHA-1 digest numbers are listed on the Apple Download web page about the software.

To verify a software update from Apple that contains a SHA-1 digest:

1. Open Terminal.
2. Type the following:

```
/usr/bin/openssl sha1 [full path to file]
```

Example:

```
/usr/bin/openssl sha1 /[full path to file]/1024SecUpd2003-03-03.dmg
```

The SHA-1 digest is displayed as:

```
sha1 ([full path to the file])= [digest]
```

Example:

```
SHA1(/Users/test/Documents/1024SecUpd2003-03-03.dmg)
    =2eb722f340d4e57aa79bb5422b94d556888cbf38
```

3. Compare the digest from the Apple web page with the digest of the downloaded image to make sure they match.

For more information, see this article on the Apple Knowledge Base: http://docs.info.apple.com/article.html?artnum=75510

Step 1: Install Mac OS X version 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, or 10.3.5

Use the installation discs for Mac OS X version 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, or 10.3.5 to install the software.

To install Mac OS X:

1. Turn on the computer and insert the first Mac OS X install disc.
2. Restart the computer while holding down the C key.

   The computer starts up from the install disc. You can release the C key when you see the Apple logo.
3. Proceed through the Installer's panes by following the onscreen instructions.
4. When the Select Destination pane appears, select the volume where you want to install Mac OS X.
5. Click Options, then click Erase and Install.

   The destination volume will be completely erased before Mac OS X is installed on it.
6. Choose Mac OS Extended (Journaled) from the "Format disk as:" pop-up menu.
7. The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc when prompted.

Step 2: Perform initial setup using Setup Assistant

The Setup Assistant program opens automatically after you install Mac OS X version 10.3. Setup Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.

When setup is complete, the computer restarts automatically. Now you can log in as the administrator user created during setup and continue with the next step.

Step 3: Install Mac OS X version 10.3.6 Update

To update Mac OS X 10.3, 10.3.1,10.3.2, 10.3.4 to Mac OS X 10.3.6 you need the MacOSXUpdateCombo10.3.6.dmg image file.

To update Mac OS X 10.3.5 to Mac OS X 10.3.6 you need the MacOSXUpdate10.3.6.dmg image file.

To install Mac OS X 10.3.6 update:

1. Insert the disk that contains the Mac OS X Update 10.3.6 .dmg file and open the file.
2. After the Mac OS X 10.3.6 update volume is mounted and opens, open the Mac OS X Update10.3.6 file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.
4. After installation is complete, click Restart and continue with the next step.

Step 4: Install the Common Criteria Tools software

Lastly, you need to install the Common Criteria Tools software.

To install the Common Criteria Tools software:

1. Insert the disk that contains the Common Criteria Tools disk image (.dmg) file and open the file.
2. After the Common Criteria Tools volume is mounted and opens, open the Common Criteria Tools package (.pkg) file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password of the administrator account you created while installing Mac OS X.
4. Follow the instructions in Chapter 3, "Setting Up the Common Criteria Configuration," on page 29.

Installing the Latest version of Mac OS X Server

The instructions in this section tell you how to install the latest Mac OS X Server with the Common Criteria Tools.

Note: The instructions in this section cover installing software on a server that, at least for the duration of the installation process, has a keyboard and display attached and has an optical drive (internal or external). It is possible to install the software on a server that does not have a keyboard, display, or optical drive. For information on installing software remotely from an administrator computer, see the getting started guide included with Mac OS X Server version 10.3 or later.

What You Need

You need the following installation software to install the Mac OS X Server version 10.3.6 or later and the Common Criteria Tools:

- **Installation discs for Mac OS X Server version 10.3 or later**
  Use the installation discs included with your Xserve system or with your copy of Mac OS X Server. (You'll update to the latest version of Mac OS X Server during the following procedure.)

  Note: If your installation discs are for a Mac OS X Server version earlier than 10.3, you must obtain Mac OS X Server version 10.3 or later.

- **Common Criteria Tools disk image file**
  The Common Criteria Tools disk image (.dmg) file contains the installer for Common Criteria Tools. This disk image file is available from the Common Criteria webpage of the AppleCare Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  After downloading the Common Criteria Tools disk image file, copy it to a removable disk such as a CD-R disc, FireWire disk, or USB disk. For instructions on copying files to a recordable CD or DVD disc, search Mac Help for "Creating CDs and DVDs using the Finder."

Verifying Disk Images

To ensure the disk images you download are accurate, they include a SHA-1 digest. If a file is changed during transit, its checksum will be different. The SHA-1 digest numbers are listed on the Apple Download web page about the software.

To verify a software update from Apple that contains a SHA-1 digest:

1. Open Terminal.
2. Type the following:

```
/usr/bin/openssl sha1 [full path to file]
```

Example:

```
/usr/bin/openssl sha1 /[full path to file]/1024SecUpd2003-03-03.dmg
```

The SHA-1 digest is displayed as:

```
sha1 ([full path to the file])= [digest]
```

Example:

```
SHA1(/Users/test/Documents/1024SecUpd2003-03-03.dmg)
     =2eb722f340d4e57aa79bb5422b94d556888cbf38
```

3 Compare the digest from the Apple web page with the digest of the downloaded image to make sure they match.

For more information, see this article on the Apple Knowledge Base: http://docs.info.apple.com/article.html?artnum=75510

Step 1: Install Mac OS X Server software

Use the installation discs for Mac OS X Server version 10.3 or later to install the server software.

Note: If you're setting up a new Xserve system with Mac OS X Server version 10.3 or later preinstalled, and the server has never been started up, you can skip this step and continue at step 2, "Perform initial server setup using Server Assistant".

To install Mac OS X Server:

1 Turn on the computer and insert the first Mac OS X Server install disc.

2 Restart the computer while holding down the C key.

The computer starts up from the install disc. You can release the C key when you see the Apple logo.

3 Proceed through the Installer's panes by following the onscreen instructions.

4 When the Select Destination pane appears, select the volume where you want to install Mac OS X Server.

5 Click Options, then click Erase and Install.

The destination volume will be completely erased before Mac OS X Server is installed on it.

6 Choose Mac OS Extended (Journaled) from the "Format disk as:" pop-up menu.

7 The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc when prompted.

After installation is complete, the Installer quits automatically and you can continue with the next step, "Perform initial server setup using Server Assistant."

If you want to postpone server setup until a later time, press Command-Q. The computer shuts down. When you restart it, the server setup process begins automatically.

Step 2: Perform initial server setup using Server Assistant

The Server Assistant program opens automatically when you first start up a new Xserve or after you install Mac OS X Server version 10.3 or later. Server Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.

To set up a server for use with Common Criteria software:

1. Before configuring settings in Server Assistant's panes, fill out the Mac OS X Server worksheet.

   The worksheet and supplemental information you need is in the getting started guide that's included with Mac OS X Server version 10.3 and later. You can also obtain the worksheet and getting started guide from the Mac OS X Server website at the following address:

   http://www.apple.com/server/documentation/

2. Start up your computer if it is off.

   Server Assistant opens automatically.

3. Enter the setup data you've recorded on the worksheet as you move through Server Assistant's panes, following the onscreen instructions.

   Make sure that any DHCP or DNS servers you specify for the server you're setting up to use are running.

4. When you reach the Administrator Account pane, make sure the password you specify has at least five characters.

5. When you reach the Network Interfaces pane, leave AppleTalk unselected for each network interface.

6. When you reach the Directory Usage pane, choose Standalone Server from the pop-up menu.

7. When you reach the Services pane, select your options from only the following services: Apple file service, Mail service, Web service, WebDAV, Network time service, NetBoot service, and QuickTime Streaming service.

   Leave all other services unselected.

8. When you reach the Network Time pane, select "Use a network time server" and enter the fully qualified DNS name or IP address of the time server on your network.

9. After all setup data has been entered, Server Assistant displays a summary of the data.

10. Review the setup data you entered. Click Go Back to change it.

11. To initiate server setup, click Apply.

    When server setup is complete, the server restarts automatically. Now you can log in as the administrator user created during setup and continue with the next step.

Step 3: Update to the latest Mac OS X Server version

Apple periodically releases free updates to Mac OS X Server. In this section you will update to Mac OS X Server version 10.3.5 or later. Use one of the two procedures that follow depending on whether the server you're setting up currently has Internet access or not.

- If the server has Internet access, follow the first procedure. You'll use the Software Update feature to retrieve and install the latest update.
- If the server doesn't have Internet access, follow the second procedure. You'll use another computer to download the software update disk image file, copy it to a removable disk, and use this disk to install the update.

To update Mac OS X Server on a server with Internet access:

1. Start up the server and log in using the name and password of the administrator account.
2. Choose Apple ( ) > Software Update.

   If there are any updates available, they appear in a list.
3. If a Mac OS X Server update is listed, click its checkbox to select it, then click Install.

   Before clicking Install, you can select the checkboxes of other updates you want to install. Apple recommends selecting security updates. To see more information about a particular update, click its name.

   When the installation complete, Software Update checks the software versions again. Sometimes several updates are required before the latest version is reached.

   After you finish using Software Update, continue with step 4, "Install the Common Criteria Tools software."

To update Mac OS X Server on a server without Internet access:

1. On a computer with Internet access, download the disk image file for the latest Mac OS X Server update from the Apple Support website, then copy the file to a removable disk that's compatible with the server you're setting up.

   You can get the disk image file for the latest update from the Mac OS X Server Support webpage, which you can get to from the Apple Support website at the following address:

   http://www.apple.com/support/
2. Insert the disk that contains the disk image file for the latest Mac OS X Server update and open the file to mount the volume containing the update Installer.
3. After the volume is mounted and opens, open the update Installer, which is a package (.pkg) file.
4. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

When prompted to authenticate, enter the name and password of the administrator account you created during server setup.

Step 4: Install the Common Criteria Tools software

Lastly, you need to install the Common Criteria Tools software.

To install the Common Criteria Tools software:

1. Insert the disk that contains the Common Criteria Tools disk image file and open the file to mount the volume containing the tools Installer.
2. After the volume is mounted and opens, open the Common Criteria Tools Installer, which is a .pkg file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password of the administrator account you created earlier.
4. Follow the instructions in the next chapter, "Setting Up the Common Criteria Configuration" on page 29.

Installing the Evaluated Configuration of Mac OS X Server

The instructions in this section tell you how to install the specific version of Mac OS X Server used to certify the evaluated configuration. This is only needed to satisfy any requirements to test the specific configuration. It's recommended that you use the latest version of Mac OS X Server. For more information on the evaluated configuration, see Chapter 1, "The Common Criteria Configuration," on page 9.

Note: The instructions in this section cover installing on a server that, at least for the duration of the installation process, has a keyboard and display attached and has an optical drive (internal or external). It is possible to install the software on a server that does not have a keyboard, display, or optical drive. For information on installing software remotely from an administrator computer, see the getting started guide included with Mac OS X Server version 10.3 or later.

What You Need

You need the following installation software to install the specific version of Mac OS X Server used to certify the evaluated configuration:

- **Installation discs for Mac OS X Server version 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, or 10.3.5.**

  Use the installation discs included with your Xserve system or with your copy of Mac OS X Server.

  Note: If your installation discs are for a version of Mac OS X Server earlier than 10.3, you must obtain Mac OS X Server version 10.3 or later.

- **Mac OS X Server Update10.3.6 disk image file**
  To update Mac OS X Server 10.3, 10.3.1, 10.3.2, 10.3.3 or 10.3.4 to Mac OS X Server 10.3.6 you need the MacOSXSrvrUpdCombo10.3.6dmg image file.

  To update Mac OS X Server 10.3.5 to Mac OS X Server 10.3.6 you need the MacOSXServerUpdate10.3.6dmg image file.

  You can determine where to get this file by referring to the Common Criteria webpage of the Apple Care Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  If the Mac OS X Server Update Installer runs automatically when you download this file, close the Install Mac OS X Server Update window. If a dialog appears and prevents you from closing the window, click Cancel to dismiss the dialog.

  After downloading the Mac OS X Server update .dmg file, copy it to a removable disk such as a CD-R disc, FireWire disk, or USB disk. For instructions on copying files to a recordable CD or DVD disc, search Mac Help for "Creating CDs and DVDs using the Finder."

- **Common Criteria Tools disk image file**
  The Common Criteria Tools disk image (.dmg) file contains the installer for Common Criteria Tools. This disk image file is available from the Common Criteria webpage of the AppleCare Knowledge Base. You can find this webpage by searching for "Common Criteria" on the Apple Support website, which is located at the following address:

  http://www.apple.com/support/

  After downloading the Common Criteria Tools disk image file, copy it to a removable disk.

Verifying Disk Images

To ensure the disk images you download are accurate, they include a SHA-1 digest. If a file is changed during transit, its checksum will be different. The SHA-1 digest numbers are listed on the Apple Download web page about the software.

To verify a software update from Apple that contains a SHA-1 digest:

1. Open Terminal.
2. Type the following:

```
/usr/bin/openssl sha1 [full path to file]
```

Example:

```
/usr/bin/openssl sha1 /[full path to file]/1024SecUpd2003-03-03.dmg
```

The SHA-1 digest is displayed as:

```
sha1 ([full path to the file])= [digest]
```

Example:

```
SHA1(/Users/test/Documents/1024SecUpd2003-03-03.dmg
     =2eb722f340d4e57aa79bb5422b94d556888cbf38)
```

3 Compare the digest from the Apple web page with the digest of the downloaded image to make sure they match.

For more information, see this article on the Apple Knowledge Base: http://docs.info.apple.com/article.html?artnum=75510

Step 1: Install Mac OS X Server version 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, or 10.3.5

Use the installation discs for Mac OS X Server version 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4 or 10.3.5 to install the server software.

To install Mac OS X Server:

1 Turn on the computer and insert the first Mac OS X Server install disc.

2 Restart the computer while holding down the C key.

The computer starts up from the install disc. You can release the C key when you see the Apple logo.

3 Proceed through the Installer's panes by following the onscreen instructions.

4 When the Select Destination pane appears, select the volume where you want to install Mac OS X Server.

5 Click Options, then click Erase.

The destination volume will be completely erased before Mac OS X Server is installed on it.

6 Choose Mac OS Extended (Journaled) from the "Format disk as:" pop-up menu.

7 The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc when prompted.

After installation is complete, the Installer quits automatically and you can continue with the next step, "Perform initial server setup using Server Assistant."

If you want to postpone server setup until a later time, press Command-Q. The computer shuts down. When you restart it, the server setup process begins automatically.

Step 2: Perform initial server setup using Server Assistant

The Server Assistant program opens automatically after you install Mac OS X Server. Server Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.

To set up a server for use with Common Criteria software:

1. Before configuring settings in Server Assistant's panes, fill out the Mac OS X Server worksheet.

   The worksheet and supplemental information you need is in the getting started guide that's included with Mac OS X Server version 10.3. You can also obtain the worksheet and getting started guide from the Mac OS X Server website at the following address:

   http://www.apple.com/server/documentation/

2. Start up your computer if it is off, and Server Assistant opens automatically.
3. Enter the setup data you've recorded on the worksheet as you move through Server Assistant's panes, following the onscreen instructions.

   Make sure that any DHCP or DNS servers you specify for the server you're setting up to use are running.

4. When you reach the Administrator Account pane, make sure the password you specify has at least five characters.
5. When you reach the Network Interfaces pane, leave AppleTalk unselected for each network interface.
6. When you reach the Directory Usage pane, choose Standalone Server from the pop-up menu.
7. When you reach the Services pane, select only the following services: Apple file service, Mail service, Web service, WebDAV, Network time service, NetBoot service, and QuickTime Streaming service.

   Leave all other services unselected.

8. When you reach the Network Time pane, select "Use a network time server" and enter the fully qualified DNS name or IP address of the time server on your network.
9. After all setup data has been entered, Server Assistant displays a summary of the data.
10. Review the setup data you entered. Click Go Back if you want to change any of the settings.
11. To initiate server setup, click Apply.

    When server setup is complete, the server restarts automatically. Now you can log in as the administrator user created during setup and continue with the next step.

Step 3: Install Mac OS X Server version 10.3.6 Update

After installing Mac OS X Server, you need to install Mac OS X Server 10.3.6 Update.

To update Mac OS X Server 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4 to Mac OS X Server 10.3.6 you need the MacOSXSrvrUpdCombo10.3.6dmg image file.

To update Mac OS X Server 10.3.5 to Mac OS X Server 10.3.6 you need the MacOSXServerUpdate10.3.6dmg image file.

To install Mac OS X Server 10.3.6 Update:

1. Insert the disk that contains the Mac OS X Server update .dmg file and open the file.
2. After the Mac OS X Server 10.3.6 Update volume is mounted and opens, open the Mac OS X Server update .pkg file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password of the administrator account you created in step 2, "Perform initial server setup using Server Assistant."
4. After installation is complete, click Restart and continue with the next step.

Step 4: Install the Common Criteria Tools software

Lastly, you need to install Common Criteria Tools.

To install the Common Criteria Tools software:

1. Insert the disk that contains the Common Criteria Tools disk image (.dmg) file and open the file.
2. After the Common Criteria Tools volume is mounted and opens, open the Common Criteria Tools package (.pkg) file.
3. Click Continue, then proceed through the Installer's panes by following the onscreen instructions.

   When prompted to authenticate, enter the name and password of the administrator account you created earlier.
4. Follow the instructions in the next chapter, "Setting Up the Common Criteria Configuration" on page 29.

Setting Up the Common Criteria Configuration

3

This chapter describes the steps required to set up the Common Criteria configuration.

The tasks you do depend on whether you're setting up the Common Criteria configuration on Mac OS X or Mac OS X Server. For each task, you're told whether you need to complete part of all of it depending on the operating system you setting up.

To set up the Common Criteria configuration, log in as an administrator and do the following tasks:

Set Up System Preferences

Security

For Mac OS X do the whole task. For Mac OS X Server do all except step 5.

1. Open System Preferences and click Security.
2. If settings are dimmed, click the lock icon and type an administrator name and password.
3. Select the "Require password to wake this computer from sleep or screen saver" checkbox.
4. Select the "Require password to unlock each secure system preference" checkbox.

   Note: Skip step 5 if you're setting up Mac OS X Server. This option is not available on Mac OS X Server.
5. Select the "Disable automatic login" checkbox.

Screen Saver

Do this task for both Mac OS X and Mac OS X Server.

1. Open System Preferences and click Desktop & Screen Saver.
2. If settings are dimmed, click the lock icon and type an administrator name and password.
3. Click the Screen Saver button.

4 Select a screen saver in the list, or select the "Use random screen saver" checkbox to see a different screen saver each time the screen saver is activated.

5 Drag the "Start screen saver" slider to choose when the screen saver starts. It's recommended the screensaver time be set to 15 minutes or less, based on your organizational policy.

CDs & DVDs

Do this task for both Mac OS X and Mac OS X Server.

1 Open System Preferences and click CDs & DVDs.

2 Choose Ignore from the "When you insert a music CD" pop-up menu.

3 Choose Ignore from the "When you insert a picture CD" pop-up menu.

4 Choose Ignore from the "When you insert a video DVD" pop-up menu.

Sharing

For Mac OS X do the whole task. For Mac OS X Server do steps 1-4.

1 Open System Preferences and click Sharing.

2 If settings are dimmed, click the lock icon and type an administrator name and password.

3 Click Services.

4 Turn on Remote Login, and turn off all other services in the list.

If you're setting up Mac OS X Server, skip the next two steps.

5 Click the Firewall button.

6 If the Firewall is on click, Stop.

Accounts

Do this task for both Mac OS X and Mac OS X Server.

1 Open System Preferences and click Accounts.

2 If settings are dimmed, click the lock icon and type an administrator name and password.

3 Click Login Options and deselect "Automatically log in as."

4 Select the "Name and password" button.

5 Select the "Hide the Sleep, Restart, and Shut Down buttons" checkbox.

6 Deselect the "Enable fast user switching" checkbox.

Date & Time

Do this task for both Mac OS X and Mac OS X Server.

Date & Time preferences should be set to use a network time server to ensure correct time entries in the audit log.

Note: If you correctly configured your computer to use a network time server during setup, you don't need to perform this step.

To set Date & Time preferences to the Common Criteria configuration:

1. Open System Preferences and click Date & Time.
2. If settings are dimmed, click the lock icon and type an administrator name and password.
3. Select the "Set Date & Time automatically" checkbox. Then enter the fully qualified DNS name or IP address of the network time server for your network.

Energy Saver

Do this task for Mac OS X Server only.

1. Open System Preferences and click Energy Saver.
2. If settings are dimmed, click the lock icon and type an administrator name and password.
3. Deselect the "Restart automatically if the computer 'freezes'" checkbox.

System Setup

Directory Access

Do this task for both Mac OS X and Mac OS X Server.

1. Open Directory Access, located in Applications/Utilities.
2. If settings are dimmed, click the lock icon and type an administrator name and password.
3. Click Services and turn off all items in the list.
4. Click Apply and choose Directory Access > Quit.

Set an Open Firmware Password

Do this task for both Mac OS X and Mac OS X Server.

When Open Firmware password protection is turned on, it:

- Prevents using the C key to start up from a CD-ROM disc
- Prevents using the N key to start up from a NetBoot server
- Prevents using the T key to start up in FireWire Target Disk Mode (on computers that offer this feature)
- Prevents starting up in Verbose mode by pressing Command-V
- Prevents starting up a system in single-user mode by pressing Command-S

- Prevents resetting Parameter RAM (PRAM) by pressing Command-Option-P-R during startup
- Requires the password to use Startup Manager, accessed by pressing the Option key during startup
- Requires the password to enter commands after starting up in Open Firmware, which is done by pressing Command-Option-O-F during startup

Note: The Open Firmware password does not prevent someone with physical access to the computer from restarting it or turning it off.

Preparing a Computer for Open Firmware Password Protection

To maximize the effectiveness of the Open Firmware Password, do the following:

- In the Accounts pane of System Preferences, strictly limit administrator user status to trusted personnel.
- In the Startup Disk pane of System Preferences, select the startup device that you plan to protect, and save changes to set your startup device.

Important: If you reset the PRAM or Open Firmware, you need to reselect your startup device before resetting the Open Firmware password.

Warning: The Open Firmware password can be reset by either of the following:
- Any administrator designated in the Accounts pane of System Preferences
- A user with physical access to the inside of the computer

Setting the Open Firmware Password

To set an Open Firmware password you must be running firmware version 4.1.7 or later.

To install the Open Firmware Password application:

- Download the Open Firmware Password application from the Apple Support website at the following address:

  http://docs.info.apple.com/article.html?artnum=120095

To turn on the Open Firmware Password:

1. Open the Open Firmware Password application.
2. Click the lock to authenticate. Enter an administrator user name and password when prompted.
3. Click Change.
4. Select the "Require password to change Open Firmware settings" checkbox.
5. Type your password in the Password and Verify fields.

Important: Do not include an uppercase "U" in the password. For more information see this article on the Apple Support website, at the following address:

http://docs.info.apple.com/article.html?artnum=107666

6 Click OK. A confirmation dialog appears.

7 Click the lock to prevent further changes.

8 Choose File > Quit.

For more information on Open Firmware, see this article in the AppleCare Knowledge Base:

http://docs.info.apple.com/article.html?artnum=120095

Turn On Auditing

Do this task for both Mac OS X and Mac OS X Server.

1 Open the file `/etc/hostconfig for editing` in a text editor.

In Terminal, type:

```
sudo vi /etc/hostconfig
```

2 Create the following entry in `/etc/hostconfig` to enable auditing:

```
AUDIT=-YES-
```

Auditing will be enabled automatically when the computer starts up.

The following table shows the possible audit settings and what they do.

AUDIT setting	What it does
`AUDIT=-YES-`	enable auditing; ignore failure
`AUDIT=-NO-`	disable auditing
`AUDIT=-FAILSTOP-`	enable auditing; processes may stop if failure occurs
`AUDIT=-FAILHALT-`	enable auditing; the system will be halted if failure occurs

If the `AUDIT` entry is missing from `/etc/hostconfig`, then auditing is turned off. A failure is any occurrence that prevents audit events from being logged. For more information on editing settings files, see "Editing Settings Files" on page 106.

Disable Password Hints

Do this task for both Mac OS X and Mac OS X Server.

1 Open the `/Library/Preferences/com.apple.loginwindow.plist` file for editing in a text editor.

In Terminal, type:

```
sudo vi /Library/Preferences/com.apple.loginwindow.plist
```

2 Set the value of `RetriesUntilHint` to `0`.

Set Password Policy

Do this task for both Mac OS X and Mac OS X Server.

To set the minimum password length to 5 characters:

- Type the following in Terminal, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
pwpolicy -n /NetInfo/DefaultLocalNode -a adminusername -
    setglobalpolicy  minChars=5
```

You may use a higher number of characters if a more secure password is desired. For more information on pwpolicy, refer to the man page documentation by entering:

```
man pwpolicy
```

Set the Global umask

Do this task for both Mac OS X and Mac OS X Server.

The umask determines the level of permissions for newly created files.

1. To set the umask for all users on the system:, type the following commands in Terminal:

```
sudo defaults write /Library/Preferences/.GlobalPreferences NSUmask
    Value
```

Use one of the following values to set the permission level:

Value	Permission level
63 (octal equivalent 077)	Only the user can read newly created files.
23 (octal equivalent 027)	The user and members of their default group can read newly created files.
18 (octal equivalent 022)	All users can read newly created files.

Warning: Setting group, or all, access to files will may allow any private, or confidential information on these files to be visible to others. To prevent private files being accessed, the user should create a directory and change the permissions to restrict all but their own access.

2. Then type this command:

```
sudo chmod 644 /Library/Preferences/.GlobalPreferences.plist
```

Configure Secure Shell

Do this task for both Mac OS X and Mac OS X Server.

Configure the secure shell (ssh) by editing the `/etc/sshd_config` file. The sshd should be configured only to accept passwords.

To configure the secure shell, make the following settings in the sshd_config file:

Settings	Value
PasswordAuthentication	yes
ChallengeResponseAuthentication	no
GSSAPIAuthentication	no
HostBasedAuthentication	no
kbdInteractiveAuthentication	no
KerberosAuthentication	no
KerberosOrLocalPasswd	no
PAMAuthenticationViaKbdInt	no
PubkeyAuthentication	no
RhostsAuthentication	no
RhostsRSAAuthentication	no
RSAAuthentication	no

In the `sshd_config` file, all options are listed, but are commented out. To set the options above to the required settings, you must uncomment them and change them to the setting shown. For more information on editing settings files, see,"Editing Settings Files" on page 106.

Remove Classic

Do this task for both Mac OS X and Mac OS X Server.

The Common Criteria configuration must not have any operating system other than Mac OS X or Mac OS X Server installed. If Classic (Mac OS 9) was previously installed, you need to remove it from the system.

To remove Classic (Mac OS 9):

1 Remove the Classic preferences pane, located here:

/System/Library/PreferencePanes/Classic.prefPane

In Terminal, type:

```
sudo rm -rf '/System/Library/PreferencePanes/Classic.prefPane'
```

2 Remove the other Classic files and directories created by the installer:

- /System/Library/Classic/
- /System/Library/CoreServices/Classic Startup.app
- /System/Library/UserTemplate/English.lproj/Desktop/Desktop (Mac OS 9)

In Terminal, type:

```
sudo rm -rf '/System/Library/Classic/'
sudo rm -rf '/System/Library/CoreServices/Classic Startup.app'
sudo rm -rf '/System/Library/UserTemplate/English.lproj/Desktop/Desktop (Mac
     OS 9)'
```

3 Remove these additional files and directories:

- /Mac OS 9 Files/
- /Applications(Mac OS 9)
- /System Folder/

In Terminal, type:

```
sudo rm -rf '/Mac OS 9 Files/'
sudo rm -rf '/Applications(Mac OS 9)'
sudo rm -rf '/System Folder'
```

Restart

Do this task for both Mac OS X and Mac OS X Server.

To ensure all your configuration changes take effect:

▪ Choose Apple ( ) > Restart.

Using Mac OS X in a Secure Manner

4

This chapter discusses how to use Mac OS X in a safe and secure way.

Using Passwords in Mac OS X

Mac OS X is designed to give you the safest and most secure computing environment available. The best thing you can do to keep the information on your computer secure is to choose a good password for your user account.

There are several different types of passwords in Mac OS X:

- **User account passwords** allow users to log in to their home folders. This is often referred to as a "login password."
- **Administrator passwords** are required to perform many tasks on the computer, including setting system preferences, installing software, and administering user accounts. An administrator password is an administrator user's login password.
- **The Open Firmware password** allows you to prevent others from starting your computer using a CD or other disk with an operating system on it.

Choosing Good Passwords

Regardless of the type of password you are creating, follow these guidelines for choosing a secure password:

- Passwords should contain a minimum of 5 characters. An administrator may have set a minimum password length for the system. You will need to consult with your administrator to find the minimum number of password characters that are acceptable.
- Passwords should contain letters, numbers, and symbols in combinations that won't be easily guessed by unauthorized users. Passwords should not consist of actual words. Use a mix of uppercase and lowercase letters, numbers, punctuation, and symbols.
- Use a different password for each resource you need to protect.
- Don't provide hints for passwords.

- Don't use any information that's easy to guess, such as your address, birth date, or child's name.
- Don't share your passwords with anyone.
- Don't store your passwords in an obvious place, such as stuck to your computer, or in a file that can be accessed by others.

To avoid potential problems with your password, you should follow these additional guidelines:

- Avoid characters that can't be entered on computers the user will be using or that might require a special key combination to enter correctly on different keyboards and platforms.
- Do not use passwords that contain leading spaces or trailing spaces.
- Some remote services may require use of only ASCII characters in passwords.

Logging Out at the End of a Session

If you leave your computer unattended, the system may be vulnerable to unauthorized access by someone using your computer and username. To prevent someone accessing your computer, log out before you leave.

Logging out will end your session. You will be required to quit all running applications and save any open documents. When you return to the computer, type your login name and password to continue working.

To log out:

1. Choose Apple menu > Log Out "User" (your account name appears in the menu).
2. You may get some confirmation dialogs. Click Log Out.

Note: To log out of a remote (ssh) user session, type "exit" in the shell. This will stop the local "ssh" process.

Setting the umask for Individual Users

The umask determines the level of permissions for newly created files. To set the umask for individual users, type the following in Terminal:

```
defaults write -g NSUmask -int value
```

Use one of the following values to set the permission level:

Value	Permission level
63 (octal equivalent 077)	Only the user can read newly created files.
23 (octal equivalent 027)	User and members of their default group can read newly created files.
18 (octal equivalent 022)	All users can read newly created files.

You must log out and log back in for the umask to take effect.

Warning: Setting permissions to group, or all, will allow any private, or confidential information in these directories to be visible to others. To prevent private files being accessed the user should create a directory and restrict the permissions.

Setting Permissions for Disks, Folders, and Files

To control access to your important information, Mac OS X automatically sets permissions for disks, folders, and files. You can only change permissions to items that you own.

Be sure that the permissions set are appropriate. For most purposes files should be accessible to the other members of your group. If you have private or confidential information, the default permissions of the files may allow others to see it. To prevent others from accessing personal information, create a directory and set its permissions to "owner". Then place your confidential files into it. No other users will be allowed into the directory.

Mac OS X provides distinct permissions for three types of users:

- The "owner" of the item, which is usually the name of the person who created the item, or yourself
- Any member of the group assigned to the item by Mac OS X
- Any other user with access to the computer

There are four levels of permission:

- Read & Write allows a user to open the item to see its contents and change it.
- Read Only allows a user to open the item to see its contents, but not change the contents or copy them.
- Write Only makes a folder into a drop box. Users can copy items to the drop box, but cannot open the drop box to see its contents. Only the owner of the drop box can open it to take items out.
- No Access blocks all access to the item so that users can't open the item, change its contents, or copy its contents.

Setting Permissions in the Mac OS X interface

You can change these permissions for an item using the Info window in the Finder.

Warning: Be sure that appropriate permissions levels are set for your files to ensure that private, or confidential information is not disclosed.

To change permissions for an item:

1. Select the item you want to set permissions for, then choose File > Get Info and click Ownership & Permissions, if necessary.
2. Choose a permission for yourself from the pop-up menu at the top of the Ownership & Permissions pane. If the menu is dimmed, you don't have permission to change this setting.
3. To change permissions for the owner, group, or others, click Detail. If necessary, click the lock icon and, when prompted, enter the name and password of an administrator user of your computer.
4. Choose permissions for each type of user from the Access pop-up menus.

   If you are setting permissions for a folder or disk and you want to apply the same permissions to every item contained in the folder or disk, click "Apply to enclosed items."

Setting Permissions Using UNIX Commands

Since Mac OS X is built on a UNIX core, you can set permissions by entering UNIX commands in Terminal.

Warning: Be sure that appropriate permissions levels are set for your files to ensure that private, or confidential information is not disclosed.

Understanding UNIX Permissions

Each file or directory has 3 types of security groups:

- **Owner:** The owner or creator of the file or directory
- **Group:** The group to which the file or directory is assigned
- **All Others:** Anyone who isn't the owner or is not assigned to the group associated with the file or directory.

Each security group is assigned a code that controls that group's permissions:

- r (read) allows the user to see the item but not make changes.
- w (write) allows the user to see and make changes to the item.
- x (execute) allows the user to run scripts or programs.
- "-" (access) means access is turned off.

To view permissions for files and directories in Terminal, type the `ls -l` command. For each file or directory listed, you see the permissions, owner and group name, and file or directory name.

Examples:
The following file (-) displays read, write, and executable permissions for owner (rwx), group (rwx) and all others (rwx):

```
-rwxrwxrwx
```

The following file (-) displays read, write, and executable permissions for owner (rwx), and group (rwx), but no permissions for others (---):

```
-rwxrwx---
```

The following file (-) displays read, write, and executable permissions for owner (rwx), but no permissions for group (---) or others (---):

```
-rwx------
```

The following file (-) displays read and write, but no executable permissions for owner (rw-), group (rw-), and others (rw-):

```
-rw-rw-rw-
```

The following file (-) displays read, write, and executable permissions for owner (rwx), but only read and executable for group (r-x) and others (r-x):

```
-rwxr-xr-x
```

The following file (-) displays read, write, and executable permissions for owner (rwx), but only read for group (r--) and others (r--):

```
-rwxr--r--
```

For more information on permissions in UNIX, refer to the man page by entering:

```
man ls
```

Changing Permissions

Use the `chmod` command to change permissions for an item.

The syntax of the command is as follows:

`chmod security group change type permission file or directory`

The options for each item in the command are described below.

Security group: The person or group whose permission you are changing. Can be any of the following:

- u - user
- g - group
- o - other
- all - all

Type of change: Whether you are adding or subtracting the permission:

- "+" - add permission
- "-" - subtract permission

Permission: The permission you are changing:

- r - read
- w - write
- x - execute

File or directory: The name of the file or directory to change:

Examples:

```
chmod go-w myfile
```

Removes write access for group and others for the file myfile.

```
chmod go+rw myfile1 myfile2
```

Adds read and write access for group and others for files myfile1 and myfile2.

```
chmod ugo+rwx myfile1
```

Adds read, write, and execute for everyone for myfile1.

For more information on changing UNIX permissions, refer to the chmod man page by entering:

```
man chmod
```

Changing the Owner

Use the `chown` command to change the owner of a file or directory.

The syntax of the command is as follows:

```
chown username file or directory
```

For example, to change the owner of file1 to the user jdoe, type:

```
chown jdoe file1
```

For more information on changing UNIX ownership, refer to the `chown` man page by entering:

```
man chown
```

Changing the Group

Use the `chgrp` command to change the group of a file or directory.

The syntax of the command is as follows:

```
chgrp groupname file or directory
```

For example: to change the group of file1 and file2 to the group ateam, type:

```
chgrp ateam file1 file2
```

For more information on changing UNIX groups, refer to the `chgrp` man page by entering:

```
man chgrp
```

Administering Mac OS X in the Common Criteria Configuration

5

This chapter describes how to perform administrative tasks when using the Common Criteria configuration.

Managing Audit Log Files

If auditing is enabled, the auditing subsystem adds records of auditable events to an audit log file. The name of an audit log file consists of the date and time it was created, followed by a period, and the date and time it was terminated, for example: `20040322183133.20040322184443`.

The audit subsystem appends records to only one audit log file at any given time. The currently active file has a suffix "`.not_terminated`" instead of a date and time.

Audit log files are stored in the directories specified in the `audit_control` file.The audit subsystem creates an audit log file in the first directory specified.

When less than the '`minfree`' amount of disk space is available on the volume containing the audit log file, the audit subsystem will:

- Issue an `audit_warn` soft warning
- Terminate the current audit log file
- Create a new audit log file in the next specified directory

Once all directories specified have exceeded this '`minfree`' limit, auditing will resume in the first directory again. However, if that directory is full, an auditing subsystem failure may occur.

Administrators may also choose to terminate the current audit log file and create a new one manually using the `audit` utility. This action is commonly referred to as "rotating the audit logs."

Use `audit -n` to rotate the current log file. Use `audit -s` to force the audit subsystem to reload its settings from the `audit_control` file (this will also rotate the current log file.)

For more information on audit log files, see,"The Audit Utility" on page 61.

About Administrator Accounts

When you set up Mac OS X or Mac OS X Server, you create a user account that is also an administrator account. A person with an administrator account can create other user accounts, install software in the Applications and Library folders, and change computer settings.

When you create new user accounts, you specify whether the user is an administrator or regular user. If you don't want the user to be able to change preferences or install software on the computer, don't give the user administrator access.

To keep your computer secure, don't share an administrator name and password with anyone. Be sure to log out when you leave your computer, or set Security preferences to require a password. If you leave your computer while you're logged in, someone could sit down at your computer while you're away and make changes using your administrator privileges.

For added security, don't set an administrator to be automatically logged in when the computer starts up. If you do, someone could simply restart the computer to gain access as an administrator.

Adding a New User Account

You can create individual user accounts for each person who uses your computer. Each new user has a separate home folder and can adjust his or her own preferences without affecting other users.

To add a new user account:

1. Choose Apple ( ) > System Preferences and click Accounts.
2. If some settings are dimmed, click the lock icon and type an administrator name and password.
3. Click Add (+) and type the user's name.
4. Type a short name if you don't want to use the short name generated automatically.
5. Type the user's password in the Password and Verify boxes.
6. Click Limitations and select options to determine what the user can do with the computer.

Changing a Password

If you are the administrator of your computer, you can change your password and the password for other user accounts.

1. Choose Apple (🍎) > System Preferences and click Accounts.
2. If the lock icon is locked, you will need to click it and authenticate.
3. Choose the account you wish to change.
4. Click in the Password box and modify the password.
5. Type your new password again in the Verify box.

Deleting a User Account

If you are an administrator for your computer, you can delete user accounts on your computer that are no longer needed.

When you delete a user account, you can choose to save the user's files or delete them.

Important: If the user's account is encrypted (FileVault is turned on), turn FileVault off for the user before you delete the account. For information about turning FileVault off, search Mac OS Help for "FileVault."

To delete a user account:

1. Choose Apple (🍎) > System Preferences and click Accounts.
2. If some settings are dimmed, click the lock icon and type an administrator name and password.
3. Select the user account you want to delete, then click Delete (-).
4. Click OK to save the user's files on the computer, or click Delete Immediately to remove the user account and all the user's files.

If you saved the user's files, they are stored in a disk image in the Deleted Users folder, which is in the Users folder on your Mac OS X disk. To see the saved files, double-click the disk image in the Deleted Users folder. You can drag the disk image to the Trash to delete the files.

Setting the Default Permissions for New Files

The default access permissions assigned to all newly created files and folders are determined by the umask setting in the system's global preferences file. The global umask setting applies to all users on the computer. You can change the global umask setting by using the `defaults` utility in Terminal. For general information about using Terminal, including getting detailed information about the `defaults` utility, see Appendix E, "Using Terminal," on page 103.

To change the global umask setting:

- Enter the following command in Terminal, replacing `value` with one of the values in the table:

```
defaults write /Library/Preferences/.GlobalPreferences NSUmask value
```

Value	Permission level
63 (octal equivalent 077)	Only the user who creates a file can read it.
23 (octal equivalent 027)	The user and members of the user's primary group can read files newly created by the user.
18 (octal equivalent 022)	All users can read newly created files.

Note: A change of the global umask setting takes effect after you log out.

Warning: Setting permissions to group, or all, will allow any private, or confidential information in these directories to be visible to others. To prevent private files being accessed the user should create a directory and restrict the permissions.

Set Password Policy

To set the minimum password length to 5 characters:

- For secure passwords, you should require every password to have a minimum of 5 characters. Type the following in Terminal, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
pwpolicy -n /NetInfo/DefaultLocalNode -a adminusername -
    setglobalpolicy  minChars=5
```

You may use a higher number of characters if a more secure password is desired. For more information on pwpolicy, refer to the man page documentation by entering:

```
man pwpolicy
```

Administering User and Group Accounts With UNIX Commands

You can administer user and group accounts by using the `dscl` and other command-line utilities in Terminal. For general information about using Terminal, including getting detailed information about specific commands and utilities, see Appendix E, "Using Terminal," on page 103.

This section covers command-line procedures for:

- Adding a user account
- Removing a user account
- Modifying a user account
- Adding a new group
- Removing a group

- Adding a user to a group
- Removing a user from a group

Adding a User Account via the Command Line

You can create new user accounts by using `dscl` and other commands and utilities in Terminal. When you create a user account via the command line, you must also set values for basic attributes of a user account such as short name, long name, user ID, primary group ID, and home directory location.

By Apple convention, a new group account is created to match each new user account. The new group account has the same short name and ID number as the new user account. The following procedure includes instructions for creating a new matching group.

If you are not following Apple convention, you need to know the ID number of the user's primary group. If you need to create a group (other than the conventional group that matches the new user account), follow the instructions in "Adding a New Group via the Command Line" on page 53 before adding a new user.

To add a user account:

1 In Terminal, identify an unused user ID number by entering the following commands to display lists of assigned user ID and group ID numbers.

```
nicl . -list /users uid | awk '{print $2}' | sort -n
nicl . -list /groups uid | awk '{print $2}' | sort -n
```

After you enter each of these commands, the `nicl` utility displays a list of assigned ID numbers resembling this example:

```
-2
0
1
99
25
26
27
70
71
74
75
76
77
78
79
501
```

Important: Pick an ID number that isn't on either list and is greater than 500.

2. Invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

   ```
   dscl localhost
   ```

   In interactive mode, the `dscl` utility displays the current directory and a ">" character as a prompt. (Specifically, `dscl` displays the current directory in the directory domain, not the current directory in the file system.)

3. Change the current directory to `/NetInfo/root/Users` by entering:

   ```
   cd /NetInfo/root/Users
   ```

4. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

   ```
   auth adminusername
   ```

5. Create a new user account, replacing `jsmith` with the new user account's short name:

   ```
   create jsmith
   ```

6. Specify the path to the new user's home directory in `/Users/`:

   ```
   create jsmith home /Users/jsmith
   ```

7. Specify the new user's default UNIX shell:

   ```
   create jsmith shell /bin/bash
   ```

8. Specify the user ID, replacing `502` with the new user's ID number:

   ```
   create jsmith uid 502
   ```

9. Specify the new user's primary group ID, replacing `502` with the primary group ID:

   ```
   create jsmith gid 502
   ```

   If you're following Apple convention, use the same ID number here as in the previous step. (You'll create a new group account for this ID number in step 12.)

10. Specify the long name for the new user account, replacing `New User` with the actual long name:

    ```
    create jsmith realname "New User"
    ```

11. Review the settings of your new user account by entering the following command, replacing `jsmith` with the new user account's short name as before:

    ```
    read jsmith
    ```

    The `dscl` utility displays the settings for your new user account. They will resemble this example:

    ```
    _writers_passwd: jsmith
    _writers_picture: jsmith
    _writers_tim_password: jsmith
    AppleMetaNodeLocation: /NetInfo/root
    NFSHomeDirectory: /Users/jsmith
    ```

```
PrimaryGroupID: 502
RealName: New User
RecordName: jsmith
UniqueID: 502
UserShell: /bin/bash
```

12 Change the current directory to `/NetInfo/root/Groups`:

```
cd /NetInfo/root/Groups
```

If you're not following the Apple convention of creating a new group account to match the new user account, skip to step 17.

13 Authenticate as an administrator with your admin user name, entering your admin password when prompted:

```
auth adminusername
```

14 Create the new group account, replacing `jsmith` with the new account's short name:

```
create jsmith
```

15 Specify the group ID, replacing `502` with the ID number:

```
create jsmith gid 502
```

16 Review the settings of your new group account by entering the following command, replacing `jsmith` with the new account's short name as before:

```
read jsmith
```

The `dscl` utility displays the settings for your new group account. They will resemble this example:

```
AppleMetaNodeLocation: /NetInfo/root
PrimaryGroupID: 502
RecordName: jsmith
```

17 Quit the `dscl` utility by entering:

```
quit
```

The `dscl` utility displays Goodbye, and then the standard shell prompt appears.

18 Assign a password to the account by entering the following command, replacing `jsmith` with the new account's short name:

```
sudo passwd jsmith
```

You will be prompted for your admin password, then the new user password, and finally the new user password again (for verification).

19 Create the home directory for the new user, replacing `jsmith` with the new account's short name:

```
sudo mkdir ~jsmith
```

20 Assign ownership of the home directory to the new user and group accounts, replacing `userName` with the short name of the new user account and `groupName` with the short name of the user account's primary group account:

```
sudo chown userName:groupName ~userName
```

If you followed the Apple convention of creating a new group account to match the new user account, the short names for both are the same. If you didn't follow the Apple convention, the group whose short name you specify must exist. If it doesn't exist yet, create it as described in "Adding a New Group via the Command Line" on page 53 before doing this step.

The user account is now complete. The new user account can now be used for login.

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Removing a User Account via the Command Line

You can remove accounts by using the `dscl` utility in Terminal.

To delete a user account:

1 In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to `/NetInfo/root/Users` by entering:

```
cd /NetInfo/root/Users
```

3 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4 Delete the user account by entering the following command, replacing `jsmith` with the user account's short name:

```
delete jsmith
```

5 Quit the `dscl` utility by entering:

```
quit
```

Note: This does not remove a user's home directory and the data that may be stored there. You can use the Finder to drag a deleted user's home directory to the Trash. A user account usually has a matching group of the same name. For information on deleting this group, see "Removing a Group via the Command Line" on page 55.

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Modifying a user Account via the Command Line

You can change the value of an attribute in a user account by using the `dscl` utility in Terminal.

The following table describes user account attributes you can modify using `dscl`:

Description	Attribute
Home directory	home
Terminal Shell	shell
Real Name	realname
Primary Group ID	gid

To change a user account attribute to a new value:

1. In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

   ```
   dscl localhost
   ```

2. Change the current directory to `/NetInfo/root/Users` by entering:

   ```
   cd /NetInfo/root/Users
   ```

3. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

   ```
   auth adminusername
   ```

4. Set the user attribute to the desired value by entering the following command, replacing `jsmith` with the user account's short name, `attribute` with the name of the attribute whose value you wish to change, and `newvalue` with the value:

   ```
   create jsmith attribute newvalue
   ```

5. Quit the `dscl` utility by entering:

   ```
   quit
   ```

   For more information on using the Directory Service Command Line utility, see the man pages by entering:

   ```
   man dscl
   ```

Adding a New Group via the Command Line

You can create new group accounts by using `dscl` and other commands and utilities in Terminal. When you create a group account via the command line, you must also set values for basic attributes of a group account such as short name and group ID.

To add a group account:

1. In Terminal, identify an unused group ID number by entering the following command to display a list of assigned group ID numbers.

   ```
   nicl . -list /groups uid | awk '{print $2}' | sort -n
   ```

The `nicl` utility displays a list of assigned ID numbers resembling this example:

```
-2
0
1
99
25
26
27
70
71
74
75
76
77
78
79
501
```

Important: Pick an ID number that isn't on either list and is greater than 500.

2. Invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

   ```
   dscl localhost
   ```

3. Change the current directory to `/NetInfo/root/Groups` by entering:

   ```
   cd /NetInfo/root/Groups
   ```

4. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

   ```
   auth adminusername
   ```

5. Create the new group, replacing `officegroup` with the new group account's short name:

   ```
   create officegroup
   ```

6. Specify the group ID, replacing `600` with the primary group id

   ```
   create officegroup gid 600
   ```

7. Review the settings of your new group by entering the following command, replacing `officegroup` with the new group account's short name:

   ```
   read officegroup
   ```

   The `dscl` utility displays the settings for your new group account. They will resemble this example:

   ```
   AppleMetaNodeLocation: /NetInfo/root
   ```

```
PrimaryGroupID: 600
RecordName: officegroup
```

8 Quit the `dscl` utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Removing a Group via the Command Line

You can remove accounts by using the `dscl` utility in Terminal.

To delete a group account:

1 In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to `/NetInfo/root/Groups` by entering:

```
cd /NetInfo/root/Groups
```

3 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4 Delete the group by entering the following command, replacing `officegroup` with the group account's short name:

```
delete officegroup
```

5 Quit the `dscl` utility by entering:

```
quit
```

Adding a user to a Group via the Command Line

You can add users to a group by using the `dscl` utility in Terminal.

To add a user to a group:

1 In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to `/NetInfo/root/Groups` by entering:

```
cd /NetInfo/root/Groups
```

3 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4 Add a user to a group by entering the following command, replacing jsmith with the short name of the user account and officegroup with the short name of the group account:

```
append officegroup users jsmith
```

5 Review the new settings of the group by entering the following command, replacing officegroup with the group account's short name:

```
read officegroup
```

The dscl utility displays the settings for the group account. They will resemble this example:

```
AppleMetaNodeLocation: /NetInfo/root
GroupMembership: origuser jsmith
PrimaryGroupID: 600
RecordName: officegroup
```

6 Quit the dscl utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Removing a User from a Group via the Command Line

You can remove users from a group by using the dscl utility in Terminal.

To remove a user from a group:

1 In Terminal, invoke the interactive mode of the dscl utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to /NetInfo/root/Groups by entering:

```
cd /NetInfo/root/Groups
```

3 Authenticate as an administrator by entering the following command, replacing adminusername with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4 View the current members of the group by entering (replacing officegroup with the group account's short name):

```
read officegroup
```

The dscl utility displays the settings for the group account. They will resemble this example, which shows the group named officegroup has users jsmith, mjones, and tblack as members:

```
AppleMetaNodeLocation: /NetInfo/root
```

```
GroupMembership: mjones jsmith tblack
PrimaryGroupID: 600
RecordName: officegroup
```

5 Delete the user by entering the following command, replacing `jsmith` with the short name of the user account and `officegroup` with the short name of the group account:

```
delete officegroup users jsmith
```

6 Review the new settings of the group:

```
read officegroup
```

The `dscl` utility displays the settings for the group, showing the user you removed is no longer a group member, as in this example:

```
AppleMetaNodeLocation: /NetInfo/root
GroupMembership: mjones tblack
PrimaryGroupID: 600
RecordName: officegroup
```

7 Quit the `dscl` utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Revoking a User's Right to Access the System

There are times when it is necessary to revoke a user's ability to access the system. This involves two steps:

- Prevent the user from logging in.
- Terminate all of a user's processes. This can be done by forcing a user to log out and then killing any remaining processes or by just killing all of a user's processes.

Preventing Users From Logging In

To removing the ability of a user to log in, the administrator should use the following command

To disable a user account:

1 In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to `/NetInfo/root/Users` by entering:

```
cd /NetInfo/root/Users
```

3. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4. Disable the user by entering the following command, replacing `jsmith` with the short name of the user account:

```
change jsmith AuthenticationAuthority ;ShadowHash; ;DisabledUser;
```

5. Quit the `dscl` utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

To re-enable an account that has been disabled:

1. In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

2. Change the current directory to `/NetInfo/root/Users` by entering:

```
cd /NetInfo/root/Users
```

3. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4. Enable the user by entering the following command, replacing `jsmith` with the short name of the user account:

```
change jsmith AuthenticationAuthority ;DisabledUser; ;ShadowHash;
```

5. Quit the `dscl` utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

Terminating All of a User's Processes

After disabling the user, you need to kill all active processes that are currently running.

Important: Unconditionally killing all of a user's processes will cause the user to lose any unsaved data.

1. To command all processes to clean up and exit by entering the following command, replacing `jsmith` with the user name:

```
sudo killall -TERM -u jsmith
```

2. Wait a few seconds to allow the previous command to execute. To terminate all user processes unconditionally by entering the following command, replacing `jsmith` with the user name:

```
sudo killall -9 -u jsmith
```

For more information on terminating processes, refer to the man page documentation by entering:

```
man killall
```

Mac OS X Auditing Administrator's Guide

6

This chapter describes how to customize the audit subsystem using the command-line and file-based interfaces provided in the Common Criteria configuration.

The audit subsystem allows authorized administrators to create, read, and delete audit information regarding the Common Criteria configuration. The audit subsystem creates a log of auditable events. and allows the administrator to read all audit information from the records in a manner suitable for interpretation. The default location for these files is the `/var/audit` directory. The audit subsystem alerts the administrator to conditions such as potential audit data loss due to lack of disk space.

Tools are provided in the Common Criteria configuration for reading, sorting, creating, and modifying the audit log. These tools allow administrators to include or exclude audited events from the set of possible events, based on user identity and the success or failure of the audit.

Before you run any commands or tools on the audit subsystem, it is assumed the system has been correctly installed and configured, and auditing has been turned on. For more information see Chapter 3, "Setting Up the Common Criteria Configuration."

The Audit Utility

The audit subsystem is controlled by the `audit` utility (`/usr/sbin/audit`). This utility transitions the system in and out of audit operation.

The default configuration of the audit mechanism is controlled by a set of configuration files in `/etc/security`.

If auditing is enabled, the `/etc/rc` startup script will start the audit daemon at system startup. All the features of the daemon are controlled by the audit utility and `audit_control` file. For more information about enabling auditing, see "Turn On Auditing" on page 33.

The audit subsystem generates warnings when relevant events such as storage space exhaustion and errors in operation are recognized during audit startup or log rotation. These warnings are communicated to the `audit_warn` script, which can then communicate these events to the authorized administrator. For more information, see "audit_warn" on page 70.

Audit Startup

The system startup scripts attempt to configure auditing early in the system startup process. Audit configuration is controlled by two mechanisms:

- `/etc/hostconfig` – Defines the global state of auditing based on the presence of a line specifying:

  `AUDIT=-YES-`

The value specified here is only relevant during startup and does not affect manual attempts to start auditing.

- `/etc/security/audit_control` – Specifies the detailed settings for the audit mechanism.

Here are the possible values for the line in `/etc/hostconfig` defining the state of auditing:

AUDIT setting	What it does
AUDIT=-YES-	enable auditing; ignore failure
AUDIT=-NO-	disable auditing
AUDIT=-FAILSTOP-	enable auditing; processes may stop if failure occurs
AUDIT=-FAILHALT-	enable auditing; the system will be halted if failure occurs

If the `AUDIT` entry is missing from `/etc/hostconfig`, then auditing is turned off.

A failure is any occurrence that prevents audit events from being logged.

Audit Classes, Audit Events, and User Masks

The audit classes, events, and user masks make the configuration of audit information more manageable by allowing administrators to finely control which events are logged in audit records.

The `audit_class` file defines a number of classes that events are normally categorized under. For more information, see Appendix B, "Mac OS X Audit Event Classes," on page 79 . The `audit_event` file maps an auditable event to a particular class; the list of auditable events extends to userspace events such as `AUE_login` so it supports the capture of user-submitted audit records. For more information, see "audit_event" on page 69.

Audit flags are defined in terms of audit classes. Audit flags can be for the whole system, or specific flags can be used for a particular user. Audit flags can include or exclude classes of events from the audit record stream based on the outcome of the event. For example, the outcome could be success, failure or both. For more information see:"audit_user" on page 69.

When a user logs in, the system-wide audit flags from the `audit_control` file are combined with the user-specific audit flags (if any) from the `audit_user` file, and together establish the process preselection mask for the user. The preselection mask determines which events will generate audit records for the given user.

If the preselection mask is changed, it is recommended that you restart the computer to ensure that all components are producing audit events consistently.

Command-Line Programs

audit

Auditing is managed by the `audit` utility. The `audit` utility follows this syntax:

```
audit [-nst] [file]
```

The `audit` utility controls the state of the auditing sub-system. The optional file operand specifies the location of the `audit_control` input file. The default file is:

```
default /etc/security/audit_control
```

You can use the following options with audit:

Option	Description
-n	Forces the audit system to close the existing audit log file and rotate to a new log file in a location specified in the audit control file.
-s	Specifies that the audit system should [re]start and re-read its configuration from the audit control file. A new log file will be created.
-t	Specifies that the audit system should terminate. Log files are closed and renamed to indicate the time of the shutdown.

For more information on using `audit`, see the man pages in Terminal, by typing:

```
man audit
```

auditreduce

The `auditreduce` utility allows you to select events that have been logged in the audit records. Matching audit records are printed to the standard output in their raw binary form. If no filename is specified, the standard input is used by default. Use the `praudit` utility to print the selected audit records in human-readable form. For more information on `praudit`, see, "praudit" on page 65.

The `auditreduce` tool follows this syntax:

```
auditreduce   [-A] [-a YYYYMMDD[HH[MM[SS]]]] [-b YYYYMMDD[HH[MM[SS]]]]
              [-c flags] [-d YYYYMMDD] [-e euid] [-f egid] [-g rgid]
              [-r ruid] [-u auid] [-j id] [-m event] [-o object=value]
              [file ...]
```

You can use the following options with auditreduce:

Option	Formatting and description
`-A`	Selects all records.
`-a`	`YYYYMMDD[HH[MM[SS]]]` Selects records that occurred after or on the given date-time.
`-b`	`YYYYMMDD[HH[MM[SS]]]` Selects records that occurred before the given date-time..
`-c`	`flags` Selects records matching the given audit classes specified as a comma-separated list of audit flags. For more information on audit flags, see, "audit_control" on page 67.
`-d`	`YYYYMMDD` Selects records that occurred on a given date. Cannot be used with `-a` or `-b` option flags.
`-e`	`euid` Selects records with the given effective user.
`-f`	`egid` Selects records with the given effective group.
`-g`	`gid` Selects records with the given real group.
`-r`	`ruid` Selects records with the given real user.
`-u`	`auid` Selects records with the given audit ID.
`-j`	`id` Selects records having a subject token with matching ID.

Option	Formatting and description
-m	event Selects records with the given event name or number.
-o	object = value file = Selects records containing the given path name. file ="/usr" matches paths starting with usr. file ="~/usr" matches paths not starting with usr. msgqid = Selects records containing the given message queue id. pid = Selects records containing the given process id. semid = Selects records containing the given semaphore id. shmid = Selects records containing the given shared memory id.

Examples:
To select all records associated with effective user ID root from the

audit log /var/audit/20031016184719.20031017122634:

```
auditreduce -e root /var/audit/20031016184719.20031017122634
```

To select all setlogin(2) events from that log:

```
auditreduce -m AUE_SETLOGIN /var/audit/20031016184719.20031017122634:
```

For more information on using `auditreduce`, see the man pages in Terminal, by typing:

```
man auditreduce
```

praudit

The `praudit` utility prints the contents of the audit records. The audit records are displayed in standard output (`stdout`). If no filename is specified, standard input (`stdin`) is used by default.

The `praudit` tool uses this syntax:

```
praudit [options] audit-trail-file [....]
```

You can use `praudit` with the following options:

Option	Description
-l	Prints the entire record in the same line. If this option is not specified, every token is displayed in a different line.
-r	Prints records in their raw format. This option is separate from `-s`.
-s	Prints the tokens in their "short" form. Short ASCII representations for record and event type are displayed. This option is separate from `-r`.
del	Specifies the delimiter. The default delimiter is the comma.

If raw or shortform are not specified, tokens are printed in their long form. That is, events are displayed according to their descriptions given in `audit_event`; UIDs and GIDs are expanded to their actual ASCII representation, date and time is displayed in standard date format, and so on.

For more information on using `praudit`, see the man pages in Terminal, by typing:

```
man praudit
```

Deleting Audit Records

An administrator can clear the audit trail by deleting audit files. Administrators can delete audit files from the command line.

Example:

```
$ sudo rm /var/audit/20031016184719.20031017122634
```

Warning: The administrator should not delete the currently active audit log .

Audit Control Files

There are several text files the audit system uses to control auditing and write audit records. The default location for these files is the `/etc/security` directory.

audit_class

The `audit_class` file contains descriptions of the auditable event classes on the system. Each auditable event is a member of an event class. Each line maps an audit event mask (bitmap) to a class and a description.

Example entries in this file are:

```
0x00000000:no:invalid class
0x00000001:fr:file read
0x00000002:fw:file write
0x00000004:fa:file attribute access
0x00000080:pc:process
0xffffffff:all:all flags set
```

File Location

`/etc/security/audit_class`

For more information on using `audit_class`, see the man pages in Terminal, by typing:

```
man audit_class
```

audit_control

The `audit_control` file contains several audit system parameters. Each line of this file is of the form `parameter:value`.

You can use audit_control with the following parameters:

Parameter	Description
`dir`	The directory where audit log files are stored. There may be more than one of these entries. Changes to this entry can only be enacted by restarting the audit system. For more information on how to restart the audit system, see, "audit" on page 63.
`flags`	Specifies which audit event classes are audited for all users. For more information on how to audit events for individual users, see, "audit_user" on page 69.
`naflags`	Contains the audit flags that define what classes of events are audited when an action cannot be attributed to a specific user.
`minfree`	The minimum free space required in the directory audit logs are being written to. When the free space falls below this limit a warning will be issued.

Audit Flags

Audit flags are a comma delimited list of audit classes as defined in the `audit_class` file. Event classes may be preceded by a prefix that changes their interpretation. For more information, see, "audit_class" on page 67.

The following prefixes can be used for each class:

Prefix	Description
+	Record successful events
-	Record failed events
^	Record both successful and failed events
^+	Don't record successful events
^-	Don't record failed events

Default

The following settings appear in the default `audit_control` file:

```
dir:/var/audit
flags:lo,ad,-all,^-fc,^-cl
minfree:20
naflags:lo
```

The flags parameter above specifies the system-wide mask corresponding to login/logout events, administrative events, and all failures except for failures in creating or closing files.

File Location

`/etc/security/audit_control`

For more information on using `audit_control`, see the man pages in Terminal, by typing:

```
man audit_control
```

audit_event

The `audit_event` file contains descriptions of the auditable events on the system. Each line maps an audit event number to a name, a description, and a class. Entries are of the form:

```
eventnum:eventname:description:eventclass
```

Each eventclass should have a corresponding entry in the `audit_class` file. For more information on `audit_class`, see, "audit_class" on page 67.

Example entries in this file are:

```
0:AUE_NULL:indir system call:no
1:AUE_EXIT:exit(2):pc
2:AUE_FORK:fork(2):pc
3:AUE_OPEN:open(2):fa
```

File Location

```
/etc/security/audit_event
```

The values for the events in this file must match the values in the `bsm_kevents.h` file.

For more information on using `audit_event`, see the man pages in Terminal, by typing:

```
man audit_event
```

audit_user

The `audit_user` file specifies which audit event classes are to be audited for the given users. If specified, these flags are combined with the system-wide audit flags in the `audit_control` file to determine which classes of events to audit for that user. These settings take effect when the user logs in.

Each line maps a user name to a list of classes that should be audited and a list of classes that should not be audited.

Entries are of the form:

```
username:alwaysaudit:neveraudit
```

In this example `alwaysaudit` is a set of event classes that are always audited, and `neveraudit` is a set of event classes that should not be audited. These sets can indicate the inclusion or exclusion of multiple classes, and whether to audit successful or failed events. For more information about audit flags, see, "audit_control" on page 67.

Example entries in this file are:

```
root:lo,ad:no
jdoe:-fc,ad:+fw
```

These settings would cause login and administrative events that succeed on behalf of user root to be audited. No failure events are audited. For the user jdoe, failed file creation events are audited, administrative events are audited, and successful file write events are never audited.

File Location

`/etc/security/audit_user`

For more information on using `audit_user`, see the man pages in Terminal, by typing:

```
man audit_user
```

audit_warn

`audit_warn` runs when `auditd` generates warning messages. The default `audit_warn` is a script whose first parameter is the type of warning; the script appends its arguments to `/etc/security/audit_messages`. Administrators may replace this script with a more comprehensive one would take different actions based on the type of warning. For example, a low-space warning could result in an email message being sent to the administrator.

An example script is below:

```
#!/bin/sh
echo "Audit warning: $@ " >> /etc/security/audit_messages
```

This example script simply appends all of its arguments to the `audit_messages` file

Below is the list of warnings generated by audit_warn with their associated arguments.

Warning	Meaning
`audit_warn allhard count`	All directories listed in audit_control are completely out of space. The number of occurrences of this event is shown as `count` in the example.
`audit_warn allsoft`	All directories listed in `audit_control` have reached their "`soft`" limit.. This is the threshold value specified in the `audit_control` file for the `minfree` entry.
`audit_warn ebusy`	The `audit` system is already running.
`audit_warn getacdir dir`	The `auditd` could not write to the given directory specified in the `audit_control` file.
`audit_warn hard dir`	The given directory is completely out of space.
`audit_warn nostart`	Auditing could not be started.
`audit_warn postsigterm`	An error occurred during the `auditd` shutdown.

Warning	Meaning
`audit_warn soft dir`	Remaining space in the given directory has reached the threshold value specified in the `audit_control` file.
`audit_warn tmpfile`	The temporary audit lock file already exists. This also indicates a fatal error in `auditd` startup.

For more information on using `audit_warn`, see the man pages in Terminal, by typing:

```
man audit_warn
```

Audit Log Files

The `dir` entry in the `audit_control` file specifies where audit logs are to be stored.

Multiple `dir` entries are permitted. The log files are created with names of the form `date.date` for log files that are closed (terminated), and `date.not_terminated` for the current log file that has not been closed. The date portion of the log file name is of the form `yyyymmddHHMMSS` with the hours in 24-hour format.

Modifying the Audit System

This section describes the typical steps necessary to configure the audit system and any additional system configuration changes that should be made to support auditing.

1 Confirm auditing is turned on. You should see the following line in `/etc/hostconfig`:

```
AUDIT=-YES-
```

There are four possible settings for AUDIT:

AUDIT setting	What it does
`AUDIT=-YES-`	enable auditing; ignore failure
`AUDIT=-NO-`	disable auditing
`AUDIT=-FAILSTOP-`	enable auditing; processes may stop if failure occurs
`AUDIT=-FAILHALT-`	enable auditing; the system will be halted if failure occurs

If the `AUDIT` entry is missing from `/etc/hostconfig` then auditing is turned off.

2 Determine where the audit log files will be stored. Create the partitions and directories (`/var/audit` for example) and add these directories to the `audit_control` file. Ensure that only the administrator has permission to read from and write to this directory.

3 Create or modify the `audit_warn` script to generate the actions in response to audit messages created by the audit system.

4 Modify the audit configuration files as desired. For example, the `audit_user` file should contain entries for users that need audit event rules other than the defaults. The `flags` and `naflags` entries in the `audit_control` file should be modified to set the desired default audited events and non-attributable audited events.

5 Restart the system. You can test the auditing system before restarting by executing `/System/Library/StartupItems/Audit/Audit start` as the authorized administrator. Monitor the system log for proper startup. It is recommended that you restart so all user processes will have the proper audit information set. For more information, see "Turn On Auditing" on page 33.

Common Criteria Setup Checklist

A Appendix

This appendix contains a checklist of the steps required to set up the Common Criteria configuration.

You can keep the checklist handy to double-check your work as you set up Mac OS X and Mac OS X Server systems to meet the Common Criteria configuration. The checklist contains all the settings from Chapter 3 but it does not discuss the options and issues related to these settings in detail. It is assumed you have read and understand all the issues presented in Chapter 3, "Setting Up the Common Criteria Configuration," on page 29.

Checklist

To set up the Common Criteria configuration, log in as an administrator and do the following:

Security

Open the Security pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Select the "Require password to wake this computer from sleep or screen saver" checkbox.
X	X	Select the "Require password to unlock each secure system preference" checkbox.
X		Select the "Disable automatic login" checkbox.

For more information on Security settings, see, "Security" on page 29.

Screen Saver

Open the Desktop & Screen Saver pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Click the Screen Saver button.
X	X	Select a screen saver.
X	X	Drag the "Start screen saver" slider to 15 minutes or less.

For more information on Screen Saver settings, see “Screen Saver” on page 29.

CDs & DVDs

Open the CDs & DVDs pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Choose Ignore from the "When you insert a music CD" pop-up menu.
X	X	Choose Ignore from the "When you insert a picture CD" pop-up menu.
X	X	Choose Ignore from the "When you insert a video DVD" pop-up menu.

For more information on CDs & DVDs settings, see “CDs & DVDs” on page 30.

Sharing

Open the Sharing pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Click Services.
X	X	Turn on Remote Login, and turn off all other services in the list.
X		Click the Firewall button.
X		If the Firewall is on click, Stop.

For more information on Sharing settings, see “Sharing” on page 30.

Accounts

Open the Accounts pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Click Login Options and deselect "Automatically log in as."
X	X	Select the “Name and password” button.
X	X	Select the "Hide the Sleep, Restart, and Shut Down buttons" checkbox.
X	X	Deselect the “Enable fast user switching” checkbox.

For more information on Accounts settings, see “Accounts” on page 30.

Date & Time

Open the Date & Time pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Select the "Set Date & Time automatically" checkbox.
X	X	Enter the DNS name or IP address of a network time server.

For more information on Date & Time settings, see “Date & Time” on page 31.

Energy Saver

Open the Energy Saver pane of System Preferences and check the following settings:

Mac OS X	Mac OS X Server	Settings
	X	Deselect the “Restart automatically if the computer ‘freezes’” checkbox.

For more information on Energy Saver settings, see “Energy Saver” on page 31.

Directory Access

Open Directory Access, located in Applications/Utilities and check the following settings:

Mac OS X	Mac OS X Server	Settings
X	X	Click Services and turn off all items in the list.

For more information on Directory Access settings, see “Directory Access” on page 31.

Set an Open Firmware Password

Install the Open Firmware application and follow these steps:

Mac OS X	Mac OS X Server	Settings
X	X	In the Accounts pane of System Preferences, strictly limit administrator user status to trusted personnel.
X	X	In the Startup Disk pane of System Preferences, select the startup device that you plan to protect, and save changes to set your startup device.
X	X	Open the Open Firmware Password application and click Change.
X	X	Select the "Require password to change Open Firmware settings" checkbox.
X	X	Type your password in the Password and Verify fields.
X	X	Click the lock to prevent further changes.

For more information on setting an Open Firmware Password settings, see “Set an Open Firmware Password” on page 31.

Turn On Auditing

Create the following entry in `/etc/hostconfig` file:

Mac OS X	Mac OS X Server	Settings
X	X	`AUDIT=-YES-`

For more information on turning on auditing, see “Turn On Auditing” on page 33.

Disable Password Hints

Edit the `Library/Preferences/com.apple.loginwindow.plist` file:

Mac OS X	Mac OS X Server	Settings
X	X	Set the value of `RetriesUntilHint` to 0.

For more information on disabling password hints, see, “Disable Password Hints” on page 33.

Set Password Policy

To set password policy, open Terminal and use pwpolicy to set the minimum password length to 5 characters.

Mac OS X	Mac OS X Server	Settings
X	X	`pwpolicy -n /NetInfo/ DefaultLocalNode -a adminusername -setglobalpolicy minChars=5`

For more information on setting password policy, see, “Set Password Policy” on page 34.

Set the Global umask

To set the global umask, open Terminal and enter the following commands:

Mac OS X	Mac OS X Server	Settings
X	X	`sudo defaults write /Library/ Preferences/.GlobalPreferences NSUmask Value`

Use one of the following values to set the permission level:

Value	Permission level
63 (octal equivalent 077)	Only the user can read newly created files.
23 (octal equivalent 027)	The user and members of their default group can read newly created files.
18 (octal equivalent 022)	All users can read newly created files.

Then type this command:

Mac OS X	Mac OS X Server	Settings
X	X	`sudo chmod 644 /Library/Preferences/ .GlobalPreferences.plist`

For more information on global umask see, “Set the Global umask” on page 34.

Configure Secure Shell

Make the following settings in the sshd_config file:

Mac OS X	Mac OS X Server	Settings
X	X	PasswordAuthentication set to yes.
X	X	All other settings to no.

For more information on Secure Shell settings, see "Configure Secure Shell" on page 34.

Remove Classic

If Classic was previously installed remove it by typing the following in Terminal:

Mac OS X	Mac OS X Server	
X	X	`sudo rm -f '/System/Library/PreferencePanes/Classic.prefPane'`
X	X	`sudo rm -rf '/System/Library/Classic/'`
X	X	`sudo rm -rf '/System/Library/CoreServices/Classic Startup.app'`
X	X	`sudo rm -rf '/System/Library/UserTemplate/English.lproj/Desktop/Desktop (Mac OS 9)'`
X	X	`sudo rm -rf '/Mac OS 9 Files/'`
X	X	`sudo rm -rf '/Applications(Mac OS 9)'`
X	X	`sudo rm -rf '/System Folder'`

For more information on removing Classic, see, "Editing Settings Files" on page 106.

Restart

To ensure all your configuration changes take effect:

Mac OS X	Mac OS X Server	Settings
X	X	Choose Apple ( ) > Restart.

Mac OS X Audit Event Classes

Appendix B

The table below contains the audit event class names and descriptions.

The name of the event is used in the `audit_control` file for the `flags` and `naflags` entries, and in the `audit_user` file for the `alwaysaudit` and `never audit` fields of the user record.

Audit Event Classes

Event Name	Description
no	Null value; turns off event preselection
fr	File read, open for read
fw	File write, open for write
fa	File attribute access
fm	File attribute modify
fc	File create
fd	File delete
cl	File close
pc	Events related to processes (kill, signal, etc.)
nt	Network events
ip	System V IPC
na	Non-attributable events
ad	Administrative
lo	Login or logout
ap	Application-generated events
io	The ioctl() system call
ex	The exec() system call
ot	Miscellaneous
all	Sets the flags for all events

Audit Record Format

Appendix C

This appendix describes the format of the various audit records.

The format of the record definitions is the same as that used by BSM (http://docs.sun.com/db/doc/806-1789).

This section contains the definitions of new tokens and audit records created for Mac OS X.

Notes:

- socket-inet tokens appear only when the system parameters are valid and the socket is successfully looked up.
- socket-unix Token describes a socket for the Unix address family.

socket-unix Token

Token ID	Socket Family	Path
1 byte	2 bytes	104 bytes

- The socket token in the form of that specified in the 1995 BSM specification:

socket token

Token ID	Socket type	Local port	Local address	Remote port	Remote address
1 byte	2 bytes	2 bytes	4 bytes	2 byte	4 bytes

- The `in_addr` token contains an Internet address. This 4-byte value is an Internet Protocol address. The token has two fields: a token ID that identifies this token as an `in_addr` token and an Internet address.

in_addr token

Token ID	Internet address
1 byte	4 bytes

The `ipc_perm` token in these records will have the seq ID and key set to 0. The creator UID is the same as owner UID, and creator GID is the same as owner GID.

The audit records created of OS X are as follows:

```
accept
  system call accept see accept(2)
  event ID 33  AUE_ACCEPT
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token


add_profile
  system call add_profil
  event ID 324  AUE_ADDPROFILE
  event class pc  (0x00000080)
  audit record
     header-token
     subject-token
     return-token

auditctl
  system call auditctl
    event ID 352  AUE_AUDITCTL
    event class ad  (0x00000800)
    audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token


auditon: A_SETQCTRL
  system call auditon see auditon(2)
  event ID 146  AUE_AUDITON_SQCTRL
  event class ad  (0x00000800)
  audit record
     header-token
     argument-token  (3, "setqctrl:aq_hiwater", hiwater)
     argument-token  (3, "setqctrl:aq_lowater", lowater)
     argument-token  (3, "setqctrl:aq_bufsz", output buffer size)
     argument-token  (3, "setqctrl:aq_delay", max write delay)
     argument-token  (3, "setqctrl:aq_minfree", %min fs free)
     subject-token
```

```
     return-token

bind
  system call bind  see bind(2)
  event ID 34  AUE_BIND
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token

chflags
  system call chflags  see chflags(2)
  event ID 303  AUE_CHFLAGS
  event class fm  (0x00000008)
  audit record
     header-token
     argument-token  (2, "flags", flags)
     path-token
     [attr-token]
     subject-token
     return-token

connect
  system call connect  see connect(2)
  event ID 32  AUE_CONNECT
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token

exchangedata
  system call exchangedata
  event ID 338  AUE_EXCHANGEDATA
  event class fm  (0x00000008)
  audit record
     header-token
     path-token
     [attr-token]
     path-token
     [attr-token]
     subject-token
```

```
    return-token

fchflags
  system call fchflags see fchflags(2)
  event ID 304  AUE_FCHFLAGS
  event class fm  (0x00000008)
  audit record
     <valid file descriptor>
     header-token
     argument-token  (2, "flags", flags)
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token   (1, "no path:fd:", fd)
     argument-token  (2, "flags", flags)
     subject-token
     return-token

flock
  system call flock  see flock(2)
  event ID 314  AUE_FLOCK
  event class fm  (0x00000008)
  audit record
     <valid file descriptor>
     header-token
     argument-token  (2, "operation", operation)
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path: fd", fd)
     argument-token  (2, "operation", operation)
     subject-token
     return-token

fpathconf
  system call fpathconf see fpathconf(2)
  event ID 327  AUE_FPATHCONF
  event class fa  (0x00000004)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
```

```
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token

fstat
  system call fstat  see fstat(2)
  event ID 326  AUE_FSTAT
  event class fa  (0x00000004)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token

ftruncate
  system call ftruncate see ftruncate(2)
  event ID 330  AUE_FTRUNCATE
  event class fm  (0x00000008)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token

futimes
  system call  futimes see futimes(2)
  event ID  318  AUE_FUTIMES
  event class   (0x00000008)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
```

```
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path: fd", fd)
     subject-token
     return-token

getattrlist
  system call  getattrlist
  event ID  335  AUE_GETATTRLIST
  event class fa  (0x00000004)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

getdirentries
  system call  getdirentries  see getdirentries(2)
  event ID  328  AUE_GETDIRENTRIES
  event class fr  (0x00000001)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token

getdirentriesattr
  system call  getdirentriesattr
  event ID  337  AUE_GETDIRENTRIESATTR
  event class fa  (0x00000004)
  audit record
     <valid file descriptor>
     header-token
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token
```

```
getfh
  system call  getfh see getfh(2)
  event ID  322  AUE_GETFH
  event class fa  (0x00000004)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

getfsstat
  system call  getfsstat  see getfsstat(2)
    event ID  301  AUE_GETFSSTAT
    event class fa  (0x00000004)
    audit record
     header-token
     subject-token
     return-token

init_process
  system call  init_process
    event ID  356  AUE_INITPROCESS
    event class pc  (0x00000080)
    audit record
     header-token
     subject-token
     return-token

kdebug_trace
  system call  kdebug_trace
  event ID  325  AUE_KDBUGTRACE
  event class pc  (0x00000080)
  audit record
     header-token
     subject-token
     return-token

ktrace
  system call  ktrace  see ktrace(2)
  event ID  306  AUE_KTRACE
  event class pc  (0x00000080)
  audit record
     <valid process ID>
     header-token
     argument-token  (2, "ops", ops)
     argument-token  (3, "trpoints", trpoints)
     process-token
     path-token
     [attr-token]
```

```
      subject-token
      return-token
      <invalid process ID or filename>
      header-token
      argument-token  (2, "ops", ops)
      argument-token  (3, "trpoints", trpoints)
      argument-token  (4, "pid", pid)
      path-token
      [attr-token]
      subject-token
      return-token

loadsharedfile
  system call  load_shared_file
  event ID  347  AUE_LOADSHFILE
  event class fr  (0x00000001)
  audit record
     header-token
     argument-token  (4, "base addr", ba)
     path-token
     [attr-token]
     subject-token
     return-token

map_fd
  system call  map_fd
    event ID  357  AUE_MAPFD
    event class no  (0x00000000)
    audit record
     <valid file descriptor>
     header-token
     argument-token  (3, "va", va)
     [path-token]
     [attr-token]
     subject-token
     return-token
     <non-file descriptor>
     header-token
     argument-token  (3, "va", va)
     argument-token  (1, "no path:fd:", fd)
     subject-token
     return-token

minherit
  system call  minheri  see minherit(2)
  event ID  340  AUE_MINHERIT
  event class pc  (0x00000080)
  audit record
     header-token
     argument-token  (1, "addr", addr)
     argument-token  (2, "len", memory segment size)
```

```
     argument-token  (3, "inherit", inherit)
     subject-token
     return-token

mkfifo
  system call  mkfifo  see mkfifo(2)
  event ID  315  AUE_MKFIFO
  event class fc  (0x00000010)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

mlock
  system call  mlock  see mlock(2)
  event ID  332  AUE_MLOCK
  event class no  (0x00000000)
  audit record
     header-token
     subject-token
     argument-token  (1, "addr", addr)
     argument-token  (2, "len", memory segment size)
     return-token

mmap
  system call    mmap             see mmap(2)
  event ID       210              AUE_MMAP
  event class    no               (0x00000000)
  audit record
       <valid file descriptor>
         header-token
         argument-token           (1, "addr", segment addr)
         argument-token           (2, "len", segment length)
         [path-token]
         [attr-token]
         subject-token
         return-token
       <non-file descriptor>
         header-token
         argument-token           (1, "addr", segment addr)
         argument-token           (2, "len", segment length)
         argument-token           (1, "no path:fd:", fd)
         subject-token
         return-token
```

```
mprotect
  system call  mprotec  see mprotect(2)
  event ID  311  AUE_MPROTECT
  event class   (0x00000008)
  audit record
     header-token
     argument-token  (1, "addr", address of memory)
     argument-token  (2, "len", memory segment size)
     argument-token  (3, "protection", protection)
     subject-token
     return-token

munlock
  system call  munlock  see munlock(2)
  event ID  333  AUE_MUNLOCK
  event class no  (0x00000000)
  audit record
     header-token
     subject-token
     argument-token  (1, "addr", addr)
     argument-token  (2, "len", memory segment size)
     return-token


newsystemsharedregions
  system call  new_system_shared_regions
  event ID  349  AUE_NEWSYSTEMSHREG
  event class ot  (0x00010000)
  audit record
     header-token
     subject-token
     return-token

nfssvc
  system call  nfssvc  see nfssvc(2)
  event ID  321  AUE_NFSSVC
  event class ot  (0x00010000)
  audit record
     header-token
     subject-token
     return-token

open
  system call  open  see open(2)
    event ID  72  AUE_OPEN_R
    event class fr  (0x00000001)
    event ID  73  AUE_OPEN_RC
    event class fc,fr  (0x00000011)
    event ID  75  AUE_OPEN_RTC
    event class fc,fd,fr  (0x00000031)
    event ID  74  AUE_OPEN_RT
```

```
    event class fd,fr  (0x00000021)
    event ID  80  AUE_OPEN_RW
    event class fr,fw  (0x00000003)
    event ID  81  AUE_OPEN_RWC
    event class fr,fw,fc  (0x00000013)
    event ID  83  AUE_OPEN_RWTC
    event class fr,fw,fc,fd  (0x00000033)
    event ID  82  AUE_OPEN_RWT
    event class fr,fw,fd  (0x00000023)
    event ID  76  AUE_OPEN_W
    event class fw  (0x00000002)
    event ID  77  AUE_OPEN_WC
    event class fw,fc  (0x00000012)
    event ID  79  AUE_OPEN_WTC
    event class fw,fc,fd  (0x00000032)
    event ID  78  AUE_OPEN_WT
    event class fw,fd  (0x00000022)
    audit record
     header-token
     path-token  path provided to system call
     [path-token]  path as the kernel knows it, if valid
     [vnode-token]
     subject-token

pid_for_task
  system call  pid_for_task
    event ID  359  AUE_PIDFORTASK
    event class pc  (0x00000080)
    audit record
     header-token
     argument-token  (1, "port", target port)
     [argument-token]  (2, "pid", returned PID)
     subject-token
     return-token


pthread_kill
  system call  __pthread_kill  see pthread_kill(2)
  event ID  350  AUE_PTHREADKILL
  event class pc  (0x00000080)
  audit record
     header-token
     argument-token  (1, "thread port", thread_port)
     subject-token
     return-token

pthread_sigmask
  system call  pthread_sigmask  see pthread_sigmask(2)
  event ID  351  AUE_PTHREADSIGMASK
  event class pc  (0x00000080)
  audit record
```

```
     header-token
     subject-token
     return-token

profile
  system call  profil  see profil(2)
  event ID  305  AUE_PROFILE
  event class pc  (0x00000080)
  audit record
     header-token
     argument-token  (4, "scale", scale)
     subject-token
     return-token

ptrace
  system call  ptrace  see ptrace(2)
  event ID  302  AUE_PTRACE
  event class pc  (0x00000080)
  audit record
     <valid process ID>
     header-token
     argument-token  (1, "request", request)
     argument-token  (3, "addr", addr)
     argument-token  (4, "data", data)
     process-token
     subject-token
     return-token
     <invalid process ID>
     header-token
     argument-token  (1, "request", request)
     argument-token  (3, "addr", addr)
     argument-token  (4, "data", data)
     argument-token  (2, "pid", pid)
     subject-token
     return-token

quotactl
  system call  quotactl  see quotactl(2)
  event ID  323  AUE_QUOTACTL
  event class ad  (0x00000800)
  audit record
     header-token
     argument-token  (2, "command", cmd)
     argument-token  (3, "uid", id)
     path-token
     [attr-token]
     subject-token
     return-token

reboot
  system call  reboot  see reboot(2)
```

```
  event ID  308  AUE_REBOOT
  event class ad
  audit record
     header-token
     argument-token  (1, "howto", howto)
     subject-token
     return-token

recvmsg
  system call  recvmsg  see recvmsg(2)
  event ID  190  AUE_RECVMSG
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token

recvfrom
  system call  recvfrom  see recvfrom(2)
  event ID  191  AUE_RECVFROM
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token

resetsharedfile
  system call  reset_shared_file
  event ID  348  AUE_RESETSHFILE
  event class ot  (0x00010000)
  audit record
     header-token
     argument-token  (1, "base addr", ba)
     subject-token
     return-token

revoke
  system call  revoke  see revoke(2)
  event ID  309  AUE_REVOKE
  event class cl
  audit record
     header-token
     path-token
```

```
     [attr-token]
     subject-token
     return-token

searchfs
  system call  searchfs
  event ID  339  AUE_SEARCHFS
  event class fa  (0x00000004)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

semclose
  system call  sem_close  see sem_close(2)
  event ID  343  AUE_SEMCLOSE
  event class ip  (0x00000200)
  audit record
     header-token
     argument-token  (1, "sem", sem)
     subject-token
     return-token

semconfig
  system call  semconfig
  event ID  341  AUE_SEMCONFIG
  event class ip  (0x00000200)
  audit record
     header-token
     subject-token
     return-token

semopen
  system call  sem_open  see sem_open(2)
  event ID  342  AUE_SEMOPEN
  event class ip  (0x00000200)
  audit record
     header-token
     text-token  (semaphore name)
     argument-token  (2, "flags", flags)
     argument-token  (3, "mode", mode)
     argument-token  (4, "value", value)
     [ipc_perm-token]*
     subject-token
     return-token

semunlink
  system call  sem_unlink  see sem_unlink(2)
  event ID  344  AUE_SEMUNLINK
```

```
  event class ip  (0x00000200)
  audit record
     header-token
     text-token  (semaphore name)
     [ipc_perm-token]*
     subject-token
     return-token

setattrlist
  system call  setattrlist
  event ID  336  AUE_SETATTRLIST
  event class   (0x00000008)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

shmopen
  system call  shm_open  see shm_open(2)
  event ID  345  AUE_SHMOPEN
  event class ip  (0x00000200)
  audit record
     header-token
     text-token  (shared memory object name)
     argument-token  (2, "flags", flags)
     argument-token  (3, "mode", mode)
     [ipc_perm-token]*
     subject-token
     return-token

shmunlink
  system call  shm_unlink  see shm_unlink(2)
  event ID  346  AUE_SHMUNLINK
  event class ip  (0x00000200)
  audit record
     header-token
     text-token  (shared memory object name)
     [ipc_perm-token]*
     subject-token
     return-token

sendmsg
  system call  sendmsg  see sendmsg(2)
  event ID  188  AUE_SENDMSG
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token>if AF_INET socket
```

```
      <path token>if AF_UNIX socket
      <path token>  canonical path of socket file
      subject-token
      return-token

sendto
  system call  sendto  see sendto(2)
  event ID  184  AUE_SENDTO
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     <socket-inet token> if AF_INET socket
     <path token> if AF_UNIX socket
     <path token>  canonical path of socket file
     subject-token
     return-token

setlogin
  system call  setlogin  see setlogin(2)
  event ID  307  AUE_SETLOGIN
  event class lo  (0x00001000)
  audit record
     header-token
     [text-token]  (login name)
     subject-token
     return-token

setprivexec
  system call  setprivexec
  event ID  320  AUE_SETPRIVEXEC
  event class pc  (0x00000100)
  audit record
     header-token
     argument-token  (1, "flag", flag)
     subject-token
     return-token

setpriority
  system call  setpriority  see priority(2)
  event ID  312  AUE_SETPRIORITY
  event class pc, ot  (0x00010080)
  audit record
     header-token
     argument-token  (1, "which", which)
     argument-token  (2, "who", who)
     argument-token  (3, "priority", priority)
     subject-token
     return-token

setsid
```

```
  system call  setsID    see setsid(2)
  event ID  319  AUE_SETSID
  event class pc  (0x00000100)
  audit record
     header-token
     subject-token
     return-token

setsockopt
  system call  setsockop  see setsockopt(2)
  event ID  35  AUE_SETSOCKOPT
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     subject-token
     return-token

settimeofday
  system call  settimeofday  see settimeofday(2)
  event ID  313  AUE_SETTIMEOFDAY
  event class ad  (0x00000800)
  audit record
     header-token
     subject-token
     return-token

shutdown
  system call  shutdown  see shutdown(2)
  event ID  46  AUE_SHUTDOWN
  event class ad  (0x00000800)
  audit record
     header-token
     argument-token  (1, "fd", file descriptor)
     subject-token
     return-token

socket
  system call  socket  see socket(2)
  event ID  183  AUE_SOCKET
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "domain", d)
     argument-token  (2, "type", type)
     argument-token  (3, "protocol", protocol)
     subject-token
     return-token

socketpair
  system call  socketpair  see socketpair(2)
```

```
  event ID  317  AUE_SOCKETPAIR
  event class nt  (0x00000100)
  audit record
     header-token
     argument-token  (1, "domain", d)
     argument-token  (2, "type", type)
     argument-token  (3, "protocol", protocol)
     subject-token
     return-token

swapoff
  system call  macx_swapoff
    event ID  355  AUE_SWAPOFF
    event class ad  (0x00000800)
    audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

swapon
  system call  macx_swapon
    event ID  28  AUE_SWAPON
    event class ad  (0x00000800)
    audit record
     header-token
     argument-token  (4, "priority", priority)
     path-token
     [attr-token]
     subject-token
     return-token

sysctl
  system call  __sysctl  see sysctl(3)
  event ID  331  AUE_SYSCTL
  event class ad  (0x00000800)
  audit record
     header-token
     subject-token
     argument-token  (1, "name", name) [one for each name segment]
     [argument-token]  (5, "newval", newval) [new value is integer]
     [text-token]  [new value is a string]
     return-token

task_for_pid
  system call  task_for_pID
    event ID  358  AUE_TASKFORPID
    event class pc  (0x00000080)
    audit record
     header-token
```

```
     <valid process ID>
     argument-token  (1, "target port", target port)
     argument-token  (3, "task port", returned task port)
     process-token
     subject-token
     return-token
     <valid process ID>
     argument-token  (1, "target port", target port)
     argument-token  (2, "process", pid)
     subject-token
     return-token

truncate
  system call  truncate  see truncate(2)
  event ID  329  AUE_TRUNCATE
  event class   (0x00000008)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token

umask
  system call  umask  see umask(2)
  event ID  310  AUE_UMASK
  event class pc  (0x00000080)
  audit record
     header-token
     argument-token  (1, "new mask", numask)
     argument-token  (0, "prev mask", previous mask)
     subject-token
     return-token

undelete
  system call  undelete  see undelete(2)
  event ID  334  AUE_UNDELETE
  event class   (0x00000008)
  audit record
     header-token
     path-token
     [attr-token]
     subject-token
     return-token
```

Satisfying CAPP Requirements

This appendix explains how the utilities described in Chapter 6 satisfy the CAPP requirements listed.

FAU_SAR.2, FAU_STG.1, and FMT_MTD.1(a)

The authorized administrator can create a new audit file by invoking the `audit` tool (see "audit" on page 63) with the `-n` or the `-s` parameters. The audit trail is written into a directory that only the administrator is allowed to read from and write to.

The event of creating, deleting, or clearing the audit file is audited in the kernel through the relevant file-level operations performed on it.

The above features satisfy requirements imposed by FAU_SAR.2, FAU_STG.1, and FMT_MTD.1(a).

FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3

Authorized administrators can use the `auditreduce` tool (see "auditreduce" on page 64) to perform audit record reduction based on various criteria including the user identity. The `praudit` tool (see "praudit" on page 65) allows the presentation of that information in a manner suitable for interpretation.

The event of reading information either successfully or unsuccessfully from the audit records is audited in the kernel through the relevant file-level operations on the audit trail files.

The above features satisfy requirements imposed by FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3.

FAU_SEL.1 and FAU_MTD.1(b)

Authorized administrators can include or exclude auditable events from the set of audited events by modifying the flags parameter in the `audit_control` file (section 3.3.2). This can be further customized for a particular user by modifying that user's entry in the `audit_user` file. The format for specification of the audit flags allows for the auditing of events based on success and failure (see "audit_user" on page 69).

The event of modifying the audit configuration is audited in the kernel through the relevant file-level operations on the control files. The audit record structure maintains the preselection mask associated with a given process; any change to the user or system flags, which corresponds to the new value for the set of audited events, is reflected in the audit records within this field.

The above features satisfy requirements imposed by FAU_SEL.1 and FAU_MTD.1(b).

FAU_STG.3 and FAU_STG.4

The audit system receives notifications from the kernel when disk space is running low on a volume and/or when the current log files reach a particular size. The alerts are written to syslog and also passed as parameters to the `audit_warn` script, which notifies the administrator of the event. For more information, see "audit_warn" on page 70. There are specified behaviors that occur when the space becomes completely exhausted. For example: `FAILSTOP` or `FAILHALT`.

The above features satisfy requirements imposed by FAU_STG.3 and FAU_STG.4.

Using Terminal

This appendix describes how to use Terminal to execute UNIX commands, run UNIX utilities, and view online information about commands and utilities.

To access a UNIX shell command prompt, you open the Terminal application. In Terminal, you can enter commands and run command-line utilities. You can use the `man` command to view online documentation for most common commands.

Notation Conventions

The following conventions are used for UNIX commands and utilities throughout this book.

Summary

Notation	Indicates
`monospaced` font	A command or other terminal text
`[text_in_brackets]`	An optional parameter
`(one|other)`	Alternative parameters (type one or the other)
`underlined`	A parameter you must replace with a value
`[...]`	A parameter that may be repeated
`<anglebrackets>`	A displayed value that depends on the computer's configuration

Commands and Other Terminal Text

Commands or command parameters that you might type, along with other text that normally appears in a Terminal window, are shown in `this` font. For example,

You can use the `doit` command to get things done.

Each command you can enter is shown on a line by itself. For example,

```
doit
```

To use this command, type "doit" at the command prompt in a Terminal window, then press the Return key.

Command Parameters and Options

Most commands require one or more parameters to specify command options or the item to which the command is applied.

Parameters You Must Type as Shown

If you need to type a parameter as shown, it appears following the command in the same font. For example,

```
doit -w later -t 12:30
```

To use the command in the above example, type the entire line as shown.

Parameter Values You Provide

If you need to supply a value, its placeholder is underlined and has a name that indicates what you need to provide. For example,

```
doit -w later -t hh:mm
```

In the above example, you need to replace `hh` with the hour and `mm` with the minute, as shown in the previous example.

Optional Parameters

If a parameter is available but not required, it appears in square brackets. For example,

```
doit [-w later]
```

To use the command in the above example, type either `doit` or `doit -w later`. The result might vary but the command will be performed either way.

Alternative Parameters

If you need to type one of a number of parameters, they're separated by a vertical line and grouped within parentheses (|). For example,

```
doit -w (now|later)
```

To perform the command, you must type either `doit -w now` or `doit -w later`.

Using Terminal

To enter shell commands or run command-line tools and utilities, you need access to a UNIX shell prompt. Both Mac OS X and Mac OS X Server include Terminal, an application you can use to start a UNIX shell command-line session on the computer.

To open Terminal:

- Double-click the Terminal application icon in the Finder (in /Applications/Utilities) or click the Terminal icon in the dock.

Terminal presents a prompt when it's ready to accept a command. The prompt you see depends on Terminal and shell preferences, but often includes the name of the host you're logged in to, your current working directory, your user name, and a prompt symbol. For example, if you're using the default bash shell and the prompt is

```
mycomputer:~ admin$
```

you're logged in to a computer named "mycomputer" as the user named "admin" and your current directory is the admin's home directory (~).

To type a command:

- Wait for a prompt to appear in the Terminal window, then type the command and press Return.

If you get the message "command not found," check your spelling.

Correcting Typing Errors

To correct a typing error before you press Return to issue the command, use the Delete key or press Control-H to erase unwanted characters and retype.

To ignore what you have typed and start again, press Control-U.

Repeating Commands

To repeat a command, press Up Arrow until you see the command, then press Return.

To repeat a command with modifications, press Up Arrow until you see the command, press Left Arrow or Right Arrow to skip over parts of the command you don't want to change, press Delete to remove characters, type regular characters to insert them, then press Return to execute the command.

Including Paths Using Drag-and-Drop

To include a fully qualified file name or directory path in a command, stop typing where the item is required in the command and drag the folder or file from a Finder window into the Terminal window.

Commands Requiring Root or Administrator Privileges

Some commands used to manage a computer must be executed by an administrator user or the root user. If you get a message such as "permission denied," the command probably requires root privileges.

You can execute one command at a time as the root user, which is an administrator implicitly, by beginning each command with `sudo`. For example:

```
sudo passwd newuser
```

To use `sudo`, you must be logged in as an administrator.

If you haven't used `sudo` recently, you're prompted to enter the administrator password.

Getting Online Help for Commands

Onscreen help is available for most commands and utilities.

Note: Not all techniques work for all commands, and some commands have no onscreen help.

To view onscreen information about a command, try the following:

- Type the command without any parameters or options. This will often list a summary of options and parameters you can use with the command.
  Example:

  ```
  sudo dscl
  ```

- Type `man command`, where `command` is the command you're curious about. This usually displays detailed information about the command, its options, parameters, and proper use.
  Example:

  ```
  man dscl
  ```

  For help using the `man` command, type:

  ```
  man man
  ```

- Type the command followed by a `-help`, `-h`, `--help`, or `help` parameter.
  Examples:

  ```
  chown help
  vi -h
  mkdir --help
  ```

Editing Settings Files

Files containing audit settings can be edited with any text editor. Terminal may be used in conjunction with Vi or emacs text editor tools included with Mac OS X.

For more information on using text editors with Terminal, see the vi or emacs man pages by entering:

```
man vi
```

or

```
man emacs
```

CAPP Requirements for the Audit Tools

This appendix describes the Common Criteria requirements related to the various audit tools.

FAU_SAR.1 Audit Review

- FAU_SAR.1.1 The TSF shall provide authorized administrators with the capability to read all audit information from the audit records.
- FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted Audit Review

- FAU_SAR.2.1 the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable Audit Review

- FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on the following attributes
- User Identity

FAU_SEL.1 Selective Audit

- FAU_SEL.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
  - User Identity
  - Success and Failure

FAU_STG.1 Protected Audit Trail Storage

- FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.
- FAU_STG.1.1 The TSF shall be able to prevent modifications to the audit records

FAU_STG.3 Action in Case of Possible Audit Data Loss

- FAU_STG.3.1 The TSF shall generate an alarm to the authorized administrator if the audit trail exceeds 80% capacity.

FAU_STG.4 Prevention of Audit Data Loss

- FAU_STG.4.1 The TSF shall be able to prevent auditable events except those taken by the authorized administrator, and overwrite old records if the audit trail is full.

FMT_MTD.1(a) Management of the audit trail

- FMT_MTD.1.1(a) The TSF shall restrict the ability to create, delete and clear the audit trail to authorized administrators.
- FMT_MTD.1(b) FMT_MTD.1.1(b) The TSF shall restrict the ability to modify or observe the set of audited events to authorized administrators